VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRIA EN EVALUACION Y AUDITORIA EN EVALUACION Y AUDITORIA DE SISTEMAS TECNOLOGICOS

III PROMOCION

TESIS DE GRADO DE MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TEMA: "ANÁLISIS FORENSE A PAQUETES DE DATOS EN LA RED LAN DE LA UNIVERSIDAD TECNOLÓGICA EQUINOCCIAL COMO APORTE AL CUMPLIMIENTO DE LAS NORMAS PCI-DSS"

AUTORES: CHUMI SARMIENTO, WILLIAM CARLOS
FLORES ESCOBAR, JOFFRE DANIEL

DIRECTOR: ING. RON EGAS, MARIO

SANGOLQUÍ, JUNIO 2014

UNIVERSIDAD DE LAS FUERZAS ARMADAS

ESPE

MAESTRIA EN EVALUACION Y AUDITORIA EN EVALUACION Y AUDITORIA DE SISTEMAS TECNOLOGICOS

CERTIFICADO DE TUTORIA

Ing. Mario Ron Msc.

CERTIFICO

Que el trabajo titulado “ANÁLISIS FORENSE A PAQUETES DE DATOS EN LA RED LAN DE LA UNIVERSIDAD TECNOLÓGICA EQUINOCCIAL COMO APORTE AL CUMPLIMIENTO DE LAS NORMAS PCI-DSS” realizado por Ing. William Chumi e Ing. Daniel Flores, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas de la Universidad de las Fuerzas Armadas-ESPE.

Debido a que la tesis contiene información confidencial de número de tarjetas de crédito no recomiendan su publicación.

El mencionado trabajo consta de 1 documento empastado y 1 disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan a Ing. William Chumi e Ing. Daniel Flores que lo entregue a Dra. Amparo Martínez Phd., en su calidad de Director de la Carrera.

Quito, Junio 2014

Ing. Mario Ron

DIRECTOR

UNIVERSIDAD DE LA FUERZAS ARMANDAS-ESPE

MAESTRIA EN EVALUACION Y AUDITORIA EN EVALUACION Y AUDITORIA DE SISTEMAS TECNOLOGICOS

DECLARACIÓN DE RESPONSABILIDAD

Ing. William Chumi S. e Ing. Daniel Flores E.

DECLARAMOS QUE:

El proyecto de grado denominado “ANÁLISIS FORENSE A PAQUETES DE DATOS EN LA RED LAN DE LA UNIVERSIDAD TECNOLÓGICA EQUINOCCIAL COMO APORTE AL CUMPLIMIENTO DE LAS NORMAS PCI-DSS”, ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan el pie de las páginas correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Quito, Junio 2014

Ing. William Chumi S.

Ing. Daniel Flores E.

UNIVERSIDAD DE LAS FUERZAS ARMADAS

ESPE

MAESTRIA EN EVALUACION Y AUDITORIA EN EVALUACION Y AUDITORIA DE SISTEMAS TECNOLOGICOS

AUTORIZACIÓN

Nosotros, Ing. William Chumi e Ing. Daniel Flores

Autorizamos a la UNIVERSIDAD DE LA FUERZAS ARMANDAS-ESPE, la publicación, en la biblioteca virtual de la Institución del trabajo Análisis Forense a paquetes de datos en la red LAN de la Universidad Tecnológica Equinoccial como aporte al cumplimiento de las normas PCI-DSS, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Quito, Junio 2014

Ing. William Chumi S.

Ing. Daniel Flores E.

UNIVERSIDAD DE LAS FUERZAS ARMADAS

ESPE

MAESTRIA EN EVALUACION Y AUDITORIA EN EVALUACION Y AUDITORIA DE SISTEMAS TECNOLOGICOS

CERTIFICADO

Ing. Mario Ron e Ing. Estevan Gómez

CERTIFICAN

Que el trabajo titulado Análisis Forense a paquetes de datos en la red LAN de la Universidad Tecnológica Equinoccial como aporte al cumplimiento de las normas PCI-DSS realizado por Ing. William Chumi e Ing. Daniel Flores, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas de la Universidad de las Fuerzas Armadas-ESPE.

Debido a que la tesis contiene información confidencial de número de tarjetas de crédito no recomiendan su publicación.

El mencionado trabajo consta de 1 documento empastado y 1 disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan a Ing. William Chumi e Ing. Daniel Flores que lo entregue a Dra. Amparo Martínez Phd., en su calidad de Director de la Carrera.

Quito, Junio 2014

Ing. Mario Ron

DIRECTOR

Ing. Estevan Gómez

CODIRECTOR

DEDICATORIA

Dedico este trabajo a mi madre, hermanos y abuelita quienes han sido los pilares de mi vida, ejemplo de esfuerzo, lucha y sacrificio.

"Si el presente es de lucha, el futuro es nuestro."

Daniel Flores Escobar

DEDICATORIA

A Dios

Por haberme dado la oportunidad de vivir y estar junto a él en cada fase de mi vida, dándome mucha paciencia para culminar con éxito este anhelado proyecto.

A mis Padres

A ellos porque son dos pilares fundamentales en mi vida, sin ellos no hubiera podido conseguir o logrado mis metas. Su perseverancia y lucha incansable han hecho de ellos un ejemplo a seguir para mí y toda mi familia.

A mis hermanos

A ellos por darme su apoyo incondicional y motivarme a la culminación de este proyecto.

William Chumi Sarmiento

AGRADECIMIENTO

Agradezco a Dios por permitirme alcanzar esta meta y ser mi luz capaz de iluminar todo momento sombrío.

A mi madre y hermanos quienes me dan su apoyo, guía y comprensión sin condición ni medida.

A todos mis familiares por su apoyo en todo momento, en especial a Yoly y Patty quienes incondicionalmente han sabido estar junto a mí

A mi amigo de tesis con quien se trabajó duro para que este trabajo culmine exitosamente. A los tutores por la ayuda prestada en el desarrollo de este proyecto.

Y a todas las personas que sin querer omito por el apoyo, ánimo y compañía en todas las diferentes etapas de mi vida. Sin importar donde estén quiero darles las gracias por formar parte de mí y por todo lo que me han brindado.

Daniel Flores Escobar

AGRADECIMIENTO

Doy las gracias a Dios por guiarme y darme la fuerza para seguir adelante y culminar todos mis anhelos ya que sin él, nada sería posible.

Agradezco al Ing. José Julio Cevallos. Rector de la Universidad Tecnológica Equinoccial por brindarme su apoyo y la facilidad de poder trabajar en la institución para el desarrollo de este proyecto.

Agradezco al Ing. Juan Carlos Rivera, Director del Instituto de Informática y Ciencias de la Computación (IDIC) y al Ing. Wilton Largo Jefe del Area Técnica del IDIC por su apoyo y por permitirme trabajar dentro del instituto para el desenvolvimiento de este proyecto.

Agradezco a los Departamentos de Tesorería y Contabilidad de la Universidad Tecnológica Equinoccial por facilitarme la información que se necesitaba para el desarrollo de este proyecto y por la paciencia que tuvieron para cada explicación que necesitaba.

Agradezco a cada uno de los docentes de la ESPE que impartieron sus conocimientos y experiencias en cada módulo de la Maestría que ayudaron de una u otra forma al desenvolvimiento de este proyecto.

A mi compañero de la tesis siendo una excelente persona formamos un grupo sólido y responsable para el desarrollo de este trabajo.

Y a todos mis amigos (as) y compañeros (as) que me incentivaron y me apoyaron para seguir esta maestría y para la culminación de este proyecto.

William Chumi Sarmiento

INDICE GENERAL

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

RESUMEN

Este trabajo no solo representa un análisis forense al interior de la Universidad Tecnológica Equinoccial, sino también una idea aproximada del estado actual en el que se encuentra la institución educativa como institución participante en el procesamiento, transmisión o almacenamiento de información de tarjetas de crédito en la aplicación del estándar Payment Card Industry – Data Security Standard (PCI - DSS), la cual tiene como finalidad la reducción del fraude relacionado con las tarjetas de crédito e incrementar la seguridad de estos datos. Previamente se realizó una evaluación en base a los requisitos que expone la norma para determinar el nivel de cumplimiento de la institución a nivel general de todos los controles de la norma PCI – DSS, teniendo en cuenta que el estándar se compone de controles físicos, lógicos y documentales. Luego del cual se realizó una búsqueda potencial de datos de tarjetas de crédito siendo esta la labor más importante ya que el núcleo del estándar es la protección de datos de tarjetas de crédito procesados, almacenados o transmitidos a través de la red, para lo cual se utilizó herramientas OpenSource para la identificación de datos de tarjeta de crédito en tráfico a través de la red LAN no cifrados ni encriptados con lo cual se determinó que la institución no cumple diferentes requisitos de la norma. Finalmente se generó un plan de acción basados en la norma para la ejecución dentro de la Universidad y gestionar los riesgos identificados.

PALABRAS CLAVES

PCI-DSS

Análisis Forense

Tarjetas de Crédito

Redes Lan

Encriptación

ABSTRACT

This work represents not only a forensic analysis into the Universidad Tecnológica Equinoccial but also a rough idea of the current state of the educative institution, as a participant institution in the processing, transmission, or storage of information related to credit cards, in the application of the standard Payment Card Industry – Data Security Standard (PCI-DSS), which has the purpose of reducing credit card fraud and increasing data security. An evaluation based on the requisites set by the standard was previously done to determine the level of attainment of the institution on a general level to all the controls of the norm PCI – DSS, taking in consideration that this standard consists of physical, logical, and documental controls. A potential research of credit card data was then done as this was the most important task since the main focus of the standard is the protection of credit card data that has been processed, stored, or transmitted through the internet. OpenSource tools were used to identify non-encoded and unencrypted credit card data that was trafficking through the LAN; it was then determined that the Institution does not comply with several requisites of the norm. Finally, a plan of action based on the standards was made to be executed within the University and to manage the identified risks.

KEY WORDS

PCI-DSS

Forensic Analysis

Credit Card

Lan Networks

Encryption

CAPITULO I

1.1. Introducción

Dentro de la Universidad Tecnológica Equinoccial no se ha presentado ataques ni fraudes al sistema de cobro con tarjetas de crédito, pero si se han presentado intromisiones de hackers hacia diferentes módulos del sistema de la universidad dejando ver que existen falencias de seguridad en la red de la institución, por lo que con el desarrollo del proyecto se pretende realizar un análisis forense preventivo.

Este proyecto de tesis tiene como propósito realizar un análisis a la red LAN de la Universidad Tecnológica Equinoccial UTE apoyados en la norma PCI-DSS, para detectar la información involucrada en los pagos de tarjeta de crédito que realizan las personas sobre los servicios que brinda la Universidad a la sociedad, determinando cuales son los riesgos y amenazas a los que se encuentra expuesto el usuario, y el impacto que se puede producir en el caso de que llegara a suceder estos eventos.

Para ejecutar estas acciones se utilizará herramientas manuales o automatizadas como expone la norma PCI-DSS y, basándonos en las mejores prácticas para el análisis forense a redes de datos. Para la aplicación de este proyecto nos apoyaremos en una metodología experimental que es la que más se acopla al desarrollo de este proyecto dentro del análisis forense, y basados en los requisitos 10 y 11 de la Norma PCI-DSS que nos guiará para la aplicabilidad de la norma. De los resultados obtenidos se generará informes con planes de acción que contengan estrategias de protección preventivas, correctivas y detectivas para mitigar el impacto de los riesgos basadas en las mismas normas.

Con esto se generarán políticas de seguridad de la información con el objetivo de preservar las características de disponibilidad, integridad y confidencialidad.

1.2. Justificación e Importancia

Con el crecimiento de las redes de comunicación que proporcionan servicios cada vez más indispensables, se ha hecho necesario implementar mecanismos (procedimientos y técnicas) que garanticen la seguridad de la información.

Además con el rápido crecimiento en la industria de las tarjetas de crédito dentro del país y a la par el aprovechamiento de delincuentes informáticos (hackers) que ingresan arbitrariamente a redes para obtener información de tarjetas de crédito y sus tarjeta habientes, se ha visto la necesidad de implementar normas de seguridad estrictas para el pago de transacciones con tarjeta de crédito haciendo a estas más seguras para los consumidores.

Ya que el problema no es que el usuario no aplique las medidas de seguridad emitidas por las entidades financieras y de control, como la Superintendencia de Bancos y Seguros SBS, sino que existen varios inconvenientes entre las cuales tenemos: la información que se almacena dentro de las bases de datos de las empresas que utilizan las tarjetas de crédito como una forma de cobro de sus productos y servicios, porque constituye una ventana abierta para la fuga de información, o que esta información sea capturada en medio de su transmisión por las redes de las entidades.

Esto quiere decir que los delincuentes informáticos pueden tener acceso a la información sin tener siquiera acceso o contacto con el documento original (tarjeta magnética). Pero esta alerta sobre la falta de protección, también respecto al manejo y almacenamiento de información, no solo es en el país sino en la mayor parte del mundo.

Porque más que recursos, lo que falta en los grupos delincuenciales para hacer daño masivamente es decisión. Actualmente, solo haría falta el equipo tecnológico para que se colecten los datos personales, claves e información financiera de cientos de miles de usuarios del sistema bancario nacional y hacer transacciones con las tarjetas de crédito.

Actualmente la Universidad no cuenta con personal especializado en el análisis forense en redes, por lo cual se ha encontrado la necesidad de aplicar el análisis forense basado en los requerimientos 10 y 11 de la norma PCI-DSS que sugiere para la protección de la información que se transmite por medio de la red en las transacciones realizadas con tarjeta de crédito, para plantear mejoras no solo en la detección sino en la prevención de los ingresos no permitidos a la red.

Es así que el cumplimiento de la normativa PCI-DSS que es un estándar de seguridad informática para transacciones con tarjeta de crédito, posee una norma que trata sobre la supervisión y pruebas regulares a la red la cual posee dos requisitos que indican que se requiere de una red segura y supervisada que proteja los datos de titulares de tarjetas, además de mantener medidas de gestión de vulnerabilidades y mantener políticas de seguridad de la información.

1.3. Planteamiento del Problema

La formulación del problema se basa principalmente en la siguiente pregunta con la finalidad de realizar un correcto análisis forense dentro de la universidad:

- ¿Cuáles son los indicadores que inciden en la seguridad de la red LAN basados en la Norma PCI-DSS?
- Además se puede identificar como cuestionamientos a resolver las siguientes inquietudes:
- ¿Qué datos se necesita proteger?
- ¿Cómo se maneja el flujo de datos de transacciones con tarjetas de crédito dentro de la universidad?
- ¿Dónde se encuentran los datos vitales?
- ¿Quién accede a los datos?
- ¿Qué controles se necesita implementar de los requisitos 10 y 11 para el cumplimiento de la norma PCI-DSS?

Aunque puede parecer obvio que uno necesite identificar los datos sensibles que se maneja en la transacciones financieras con tarjeta de crédito, por tal motivo en el presente proyecto de tesis se realizará un análisis para una identificación previa de las áreas donde se genera la información de las transacciones de tarjeta de crédito luego de eso identificar sectores donde podría ser más vulnerable la información de estas transacciones para posteriormente realizar un análisis a un segmento de la red LAN y la transmisión de datos dentro del mismo segmento en la Universidad Tecnológica Equinoccial apoyado en los requerimientos 10 y 11 de la norma PCI-DSS con la finalidad de detectar falencias que afecten a la integridad / seguridad de la información de la Universidad, en lo que se refiere a pagos con tarjeta de crédito de los servicios que oferta dicha entidad, además de recomendar medidas de seguridad basados en la misma norma.

1.4. Alcance

En el presente trabajo se va a realizar el análisis forense a la Red Lan de la Universidad Tecnológica Equinoccial en donde se analizará y evaluará diferentes herramientas para este propósito en base a los requisitos 10 y 11 de la Normativa PCI-DSS.

Sin embargo en el presente estudio se pone a consideración de la Universidad Tecnología Equinoccial, la cual tiene la potestad de implementar el plan de acción que se entregara como aporte del presente trabajo.

1.5. Metodología

Se plantea una metodología definida para el análisis forense con las mejores prácticas con la finalidad de que el proyecto sea coherente, y lo más importante, se obtengan resultados de calidad y confiables.

Es así que para la realización de este proyecto se aplica la metodología experimental especificando como se realizó la toma de muestra y captura de datos

además de los medios utilizados para la ejecución de esta tarea, el análisis realizado a los mismos, finalmente detallando el resultado del análisis para posterior generar un plan de acción para ser aplicado.

1.6. Objetivos

1.6.1. Objetivo General

Identificar procesos y procedimientos, estructurales y funcionales a través de un análisis forense para verificar la seguridad de la información en la red LAN de la Universidad Tecnológica Equinoccial para la implementación de los requisitos 10 y 11 de la Norma PCI-DSS.

1.6.2. Objetivos Específicos

- Identificar los procesos transaccionales de la red informática dentro de la Universidad Tecnológica Equinoccial y los canales involucrados en la información de los tarjetahabientes.
- Analizar la infraestructura de la red de la UTE que soporta las transacciones que se realizan con tarjeta de crédito, cuantificando el número de transacciones que se genera con esta forma de pago.
- Determinar técnicas y herramientas de análisis forense en la transmisión de datos dentro de la red LAN de la Universidad.
- Identificar, preservar y analizar el flujo de paquetes de datos en las áreas donde se genera la transmisión de datos con información de tarjetas de crédito dentro de la Universidad.
- Evaluar la seguridad de la información trasmitida por las redes LAN, donde se genera información de las tarjetas de crédito dentro de la Universidad, basados en los requisitos 10 y 11 de la norma PCI-DSS.
- Proponer un plan de acción con los controles evaluados de los requisitos 10 y 11 de la Norma PCI-DSS.

CAPITULO II

2.1. Normas PCI-DSS

El robo de identidad, fraude y violaciones de seguridad son problemas que enfrentan los procesadores de pago, los comerciantes y proveedores de servicios en el actual entorno de procesamiento de tarjetas de crédito. Los consumidores quieren asegurarse de que sus datos de tarjeta de crédito están protegidos. Es por eso que a partir del año 2005 la industria de tarjetas de crédito está tomando medidas para mejorar la seguridad.

EL PCI Security Standards Council es un foro global abierto para el continuo desarrollo, mejora, almacenamiento, divulgación e implementación de normas de seguridad para la protección de datos de tarjeta habientes.

Su misión es mejorar la seguridad en la industria de tarjetas de pago llevando a cabo educación y concientización de las normas de seguridad PCI.

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) “se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial. Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las PCI DSS se aplican a todas las entidades que participan en los procesos de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios, así como también todas las demás entidades que almacenan, procesan o transmiten datos de titulares de tarjetas como se muestra en la Ilustración 1. Las PCI DSS constituyen un conjunto mínimo de requisitos para proteger datos de titulares de tarjetas y se pueden mejorar con el uso de controles y prácticas adicionales para mitigar otros riesgos” (Requisitos de las PCI DSS y procedimientos para la evaluación de la seguridad, versión 2.0, 2010).

Fue fundada por las 5 principales marcas de tarjetas de pago: American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa, que exigen a sus partners de negocio acogerse a su más estricto cumplimiento perdiendo, en caso de incumplimiento, la autorización para procesar sus tarjetas.

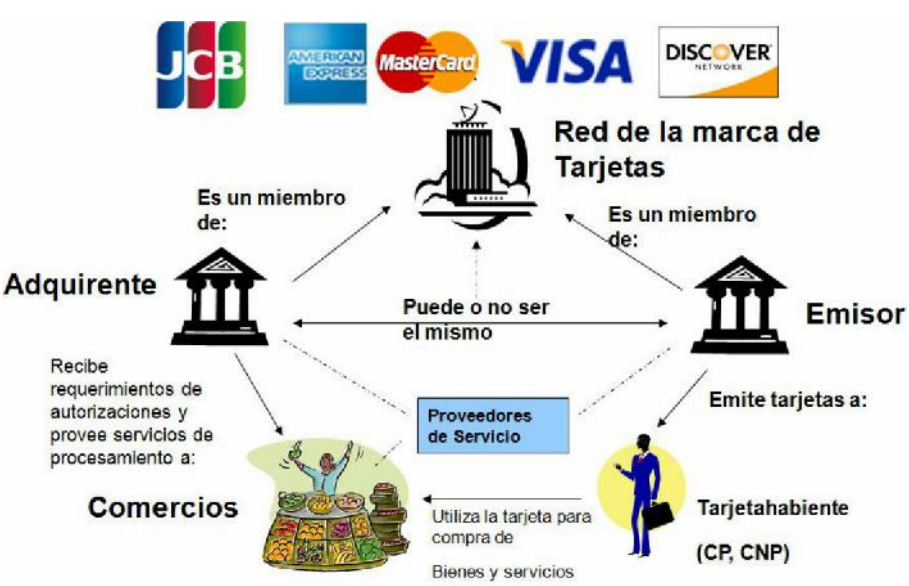


Ilustración 1 Funcionamiento Norma PCI-DSS

Fuente: http://www.blackhatconsultants.com/guides/pcidss.html

El Estándar de Seguridad de Datos (DSS) tiene como objetivo mejorar la seguridad de los datos de la tarjeta de pago. Al adherirse a la norma PCI DSS, todos los interesados pueden crear un entorno más seguro para procesar, almacenar y transmitir información de su tarjeta de crédito. Las empresas que no cumplan podrían ser objeto de multas, restricción o pérdida de privilegios de aceptación de tarjetas, por no hablar de la reputación seriamente dañada. Su cumplimiento obliga a fabricantes y suministradores de sistemas y aplicaciones a concebir y desarrollar el software de modo acorde a esas orientaciones, y a someterlas a prueba por parte de entidades validadoras que comprueben su ajuste a las regulaciones emanadas.

La norma marca seis grandes objetivos los mismos se muestran en la Ilustración 2. Y alcanzar cada uno de ellos se concretan en una docena de requerimientos que quedan sintetizados en la tabla 1

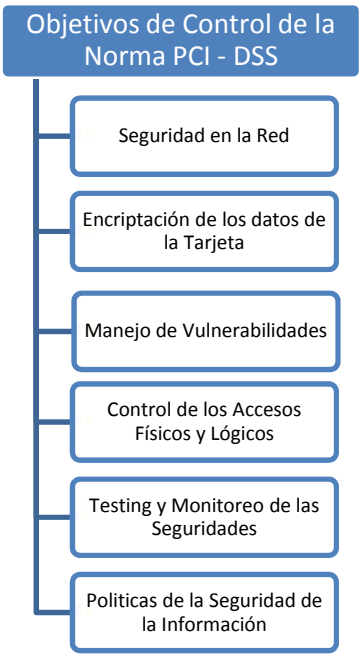


Ilustración 2 Objetivos Norma PCI-DSS

Tabla 1 Requisitos Norma PCI-DSS

Desarrolle y mantenga una red segura	
Requisito 1:	Instalar y mantener una configuración de cortafuegos para proteger los datos de los propietarios de tarjetas.
Requisito 2:	No usar contraseñas del sistema y otros parámetros de seguridad provistos por los proveedores
Proteger los datos de los propietarios de tarjetas	
Requisito 3:	Proteger los datos almacenados de los propietarios de tarjetas.
Requisito 4:	Cifrar los datos de los propietarios de tarjetas e información confidencial transmitida a través de redes públicas abiertas.
Mantener un programa de manejo de vulnerabilidad	
Requisito 5:	Usar y actualizar regularmente un software antivirus
Requisito 6:	Desarrollar y mantener sistemas y aplicaciones seguras
Implementar medidas solidas de control de acceso	
Requisito 7	Restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información

CONTINUA

Requisito 8:	Asignar una identificación única a cada persona que tenga acceso a un computador
Requisito 9:	Restringir el acceso físico a los datos de los propietarios de tarjetas
Monitorear y probar regularmente las redes	
Requisito 10:	Rastrear y monitorizar todo el acceso a los recursos de la red y datos de los propietarios de tarjetas
Requisito 11:	Probar regularmente los sistemas y procesos de seguridad
Mantener una política de seguridad de información	
Requisito 12:	Mantener una política que contemple la seguridad de la información

El primero Desarrollar y Mantener una red segura trata de garantizar la integridad del perímetro. Ello se consigue implantando políticas adecuadas en firewall y routers, sobre los que se ha de realizar un adecuado y puntual control de los cambios y configuraciones. Pero también – fuente de exposición – deben identificarse todas las conexiones de los datos sensibles con la red (incluso inalámbrica) y bloquear el tráfico improcedente originado en servidores o redes consideradas inseguras. Y para eliminar riesgos, exige prohibir el acceso a los datos de tarjetas desde internet o y disponer de cortafuegos personales en laptops que compartan el acceso a los datos con la navegación por Internet.

En cuanto a la seguridad lógica, la norma exige que no se empleen y se eliminen tanto las credenciales de acceso suministradas por defecto por los proveedores como las funciones innecesarias. Además, han de implementarse los medios de autenticación adecuados y bloquearse los accesos indebidos a la red y a los sistemas.

El segundo de los objetivos Proteger los datos del propietario de la tarjeta intenta evitar el uso no autorizado o el acceso indebido a la información de la que las entidades dispongan. Con esta finalidad obliga a tomar medidas tales como limitar la retención y disponibilidad de los datos al tiempo necesario para desarrollar las transacciones, y establecer procesos de eliminación de los mismos cuando no sean necesarios. Ordena, además, no guardar información innecesaria y

encriptar tanto al almacenarlos como al transmitirlos aquellos identificadores que puedan resultar susceptibles de empleo en actividades fraudulentas.

El tercero Mantener un programa de manejo la vulnerabilidades establece criterios de defensa y prevención. Exige el uso regular, continuado y actualizado constantemente de herramientas antivirus y antimalware tanto en servidores expuestos como en endpoints que sean susceptibles de infección. A la vez demanda el correcto mantenimiento de la seguridad en los medios de proceso mediante la implementación a su tiempo de los parches a sistemas operativos y aplicaciones, y el desarrollo de aplicaciones y programas seguros para evitar la exposición a riesgos elevados especialmente de aquellas transacciones abiertas al público.

El cuarto objetivo Implementar medidas solidas de control de acceso concreta tres necesidades (quién, qué y para qué): En primer lugar, asignar a cada persona una identificación sólida y protegida al máximo de suplantación que permita monitorizar su actividad, evitando el uso compartido de cuentas y que sea revocada y eliminada cuando ya resulte innecesaria. Ese habría de ser un paso previo necesario para filtrar el acceso a datos sensibles a quien que los precise para desarrollar su trabajo. Ha de evitarse además la proximidad física de las informaciones sensibles (incluidos accesos WiFi), con personas ajenas a la organización. Se sugiere a este fin almacenar (por ejemplo) los soportes físicos de backup en localizaciones seguras y destruir la información cuando ya no sea necesario.

Con el quinto objetivo sobre monitorización y evaluación con regularidad de las redes se pretende trazar la actividad de quien pueda/pudiera haber estado en contacto con la información sensible. Esto se consigue mediante registros de auditoría que hagan posible un estudio forense. Se prescribe también la ejecución de acciones preventivas que posibiliten detectar puntos de acceso no autorizados y fuera de control (por ejemplo, conexiones wireless), la realización de pruebas de penetración externa, y la instalación de herramientas tanto de control de

intrusiones como de validación de cambios y configuraciones en los elementos de la infraestructura.

El último de los objetivos mantener una política de seguridad de la información, que se alcanza con el desarrollo, publicación y difusión de las correspondientes regulaciones administrativas y la frecuente comprobación de que se cumplen.

PCI-DSS ha demostrado su validez a lo largo de este tiempo, logrando minimizar el número de brechas en la seguridad y estableciendo un elevado nivel de confianza de los usuarios de tarjetas de crédito en las entidades que manejan ese tipo de información.

Así mismo, en la norma PCI-DSS se ofrece una serie de recomendaciones para restringir el entorno de sistemas involucrados con datos de tarjetas de crédito. Dentro de ellas se encuentra una correcta segmentación de red, para aislar aquellos elementos que procesan, almacenan o transmiten datos de tarjetas de los que no lo hacen. Así mismo, la tercerización de los servicios y separación de información, teniendo en cuenta que cualquier elemento que no intervenga en el proceso puede ser excluido del cumplimiento de los controles, obligatorios por defecto.

2.2. Redes de Datos

Dentro de una red de cómputo existen varios tipos de elementos que la integran, estos elementos ya sea finales o intermedios, sirven de fuente de información útil para la realización de un análisis forense. Antes de utilizar cualquier herramienta de monitoreo o análisis de red, se debe entender la arquitectura general de una red de cómputo. El primer punto para los administradores de la red es saber dónde está el tráfico de interés. A continuación se describen los elementos que integran una red de cómputo como lo son firewalls, routers, IDS´s (Sistemas de Detección de Intrusos), etc. que se muestran en la Ilustración 3, con la finalidad de saber qué tipo de información y en que

dispositivos de red se pueden encontrar elementos necesarios que ayuden a realizar un análisis forense en redes de computo.

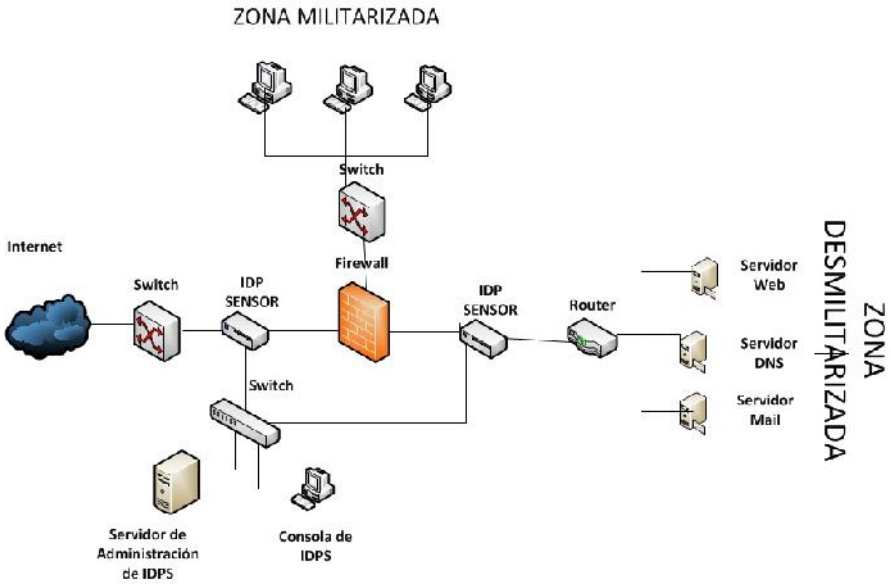


Ilustración 3 Infraestructura de la Red

El modelo TCP/IP se encuentra dividido en 5 capas que están jerarquizadas como se indican en la Ilustración 4, en cada una de ellas, sus servicios y funciones son variables para cada tipo de red. Sin embargo, en cualquier red, la misión de cada capa es proveer servicios a las capas superiores haciendo transparente el modo en que los servicios se llevan a cabo.

De esta manera, cada capa debe ocuparse exclusivamente de su nivel inmediatamente inferior, a quien solicita servicios, y del nivel inmediatamente superior, a quien devuelve resultados. Cada una de las 5 capas del protocolo TCP/IP contiene información importante. La capa de acceso al medio proporciona información acerca de componentes físicos mientras que otras capas describen los aspectos lógicos. Para identificar los eventos dentro de una red, un analista puede relacionar una dirección IP con la dirección MAC; la combinación del protocolo IP y los números de puertos pueden decirle a un analista qué aplicación se está

utilizando; esto puede ser verificado mediante el análisis de los datos de la capa de aplicación.

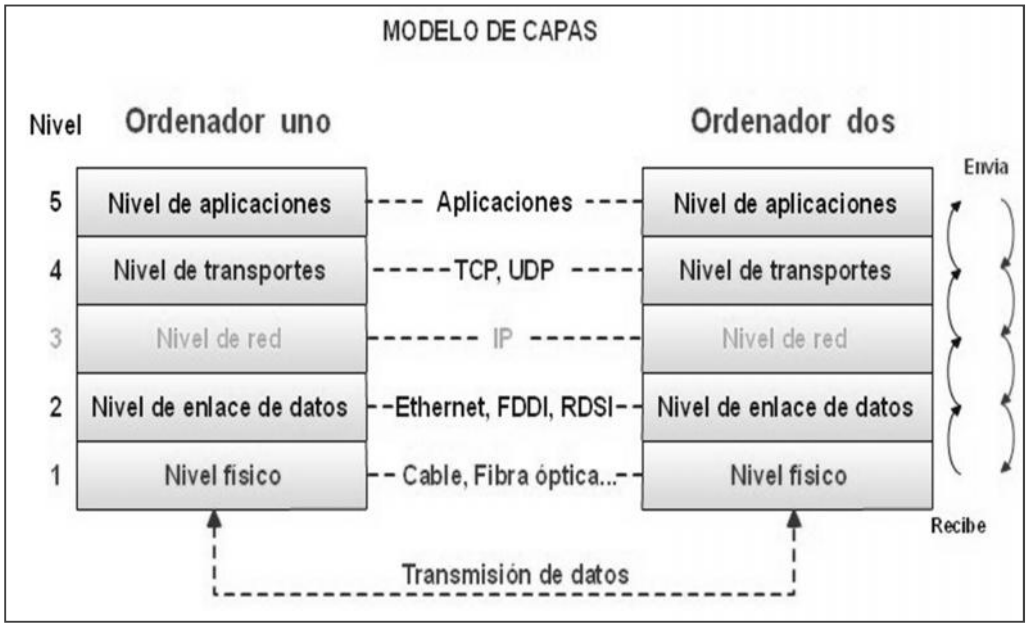


Ilustración 4 Detalle del modelo TCP/IP

Fuente: http://www.portaleso.com/usuarios/Toni/web_redes/unidad_redes_informaticas_indice.html

Cuando los analistas comienzan a examinar los datos, es típico que inicien por la dirección IP de interés y tal vez el protocolo y la información del puerto. Esta información es suficiente para apoyar la búsqueda de fuentes de datos para obtener más información. En la mayoría de los casos, la capa de aplicación contiene la actividad de interés, muchos de los atacantes encuentran las vulnerabilidades en las aplicaciones (incluidos los servicios). Los analistas tienen la necesidad de examinar las direcciones IP a fin de identificar a los usuarios que puedan haber participado en la actividad.

En la actualidad los administradores de redes se basan en los registros del IDS (Sistema de Detección de Intrusos) y del firewall para realizar un análisis forense. Pero por ejemplo en un IDS no se puede utilizar para encontrar las

víctimas de una rápida propagación de un virus. Esto se debe a que la propagación del virus es más rápida de lo que se podrían actualizar las firmas del IDS.

Los atacantes de las redes de cómputo a menudo ocultan su identidad y lugar, pero forman una cadena de conexión, acceden a un conjunto de sistemas o comprometen su identidad antes de atacar un objetivo. Un método para detectar atacantes consiste en analizar huellas de los paquetes contenidos en las conexiones que se utilizan, pudiendo ser comparadas para determinar si dos conexiones contienen el mismo texto y, por tanto, puede ser parte de la misma cadena de conexión. El método, sin embargo, falla cuando las conexiones están codificadas. Existen herramientas de captura de paquetes que se centran en capturar el tráfico de la red en bruto de una LAN (Red de Área Local) y almacenarla durante días.

2.2.1. Hardware dentro de la Red

Dentro del hardware se encuentra algunos componentes que son parte de la Red de datos:

2.2.1.1. Firewall

Un Firewall simplemente es un filtro que controla todas las comunicaciones que pasan de una red a otra y está en función de permitir o negar todo a su paso basado en un conjunto de normas dictadas por el administrador de la red. Funciona a nivel de enlace de datos como filtro con la dirección MAC, a nivel de red permite filtrados de paquetes IP (dirección origen, dirección destino), o a nivel de transporte con los puertos origen y destino. Un firewall básicamente es utilizado para realizar las siguientes funciones generales:

- Filtrado de paquetes y protocolos
- Inspección del estado de las conexiones
- Realizar la función de Proxy sobre aplicaciones seleccionadas
- Realizar NAT (Traducción de Direcciones de Red)
- Registrar el tráfico denegado

2.2.1.2. Router

Un router es un dispositivo de hardware que se utiliza para la interconexión de redes de cómputo, opera en la capa tres (nivel de red). Este dispositivo permite asegurar el tráfico de paquetes entre redes, es capaz de asignar diferentes preferencias a los mensajes que fluyen por la red y seleccionar los caminos más cortos que otros, así como, de buscar soluciones alternativas cuando un camino está saturado.

2.2.1.3. Switches

Un switch es un dispositivo de interconexión de redes de cómputo que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red, se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola.

Los switches poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un switch provoca que se almacene su dirección MAC, esto permite que la información dirigida a un dispositivo vaya desde el puerto de origen al puerto de destino, por lo tanto en el puerto de interconexión se almacenan las MAC de los dispositivos.

2.2.2. Ataques contra Redes

2.2.2.1. Inseguridad y Vulnerabilidades en la Red

En la actualidad, las aplicaciones web tienen acceso a información valiosa como números de tarjetas de crédito, información de cuentas bancarias, información clasificada, información personal entre otras.

2.2.2.2. Vulnerabilidades de la capa de red

Están estrechamente ligadas al medio sobre el que se realiza la conexión, esta capa presenta problemas de control de acceso y de confidencialidad, las vulnerabilidades a este nivel pueden ser las siguientes:

- Desvío de los cables de conexión hacia otros sistemas.
- Interceptación intrusiva de las comunicaciones (pinchar las líneas)
- Escuchas no intrusivas en medios de transmisión sin cables, etc.

2.2.2.3. Vulnerabilidades de la capa de internet

En esta capa se puede realizar cualquier ataque que afecte un datagrama IP, se incluyen como ataques contra esta capa las técnicas de:

- Sniffing,
- Suplantación de mensajes.
- Modificación de datos
- Retrasos de mensajes y denegación de mensajes

2.2.2.4. Vulnerabilidad de la capa de transporte

En esta capa podemos encontrar problemas de autenticación, de integridad y de confidencialidad, algunos de los ataques más conocidos en esta capa son:

- Las denegaciones de servicio debido a protocolos de transporte
- Interceptación de sesiones TCP establecidas (secuestro de sesiones)

2.2.2.5. Vulnerabilidad de la capa de aplicación

En esta capa contiene varias deficiencias en seguridad esto se debe a la gran variedad de protocolos que actúan en ella algunas de las debilidades se presentan en los siguientes servicios:

- Servicio de nombres de dominio
- Telnet
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)

2.3. Tarjetas de Crédito

Una Tarjeta de Crédito es un documento de plástico que contiene la identificación del usuario, así como un número asignado por el emisor de la Tarjeta, un logo de la Marca de la Tarjeta y del Emisor, además de varias seguridades, que generalmente son de uso universal ya que provienen de regulaciones internacionales emanadas por acuerdo de las principales marcas de Tarjetas de Crédito a nivel mundial (PCI Payment Card Industry). Entre las cuales tenemos en el anverso de la tarjeta:

- El nombre de la entidad emisora en la parte superior (una entidad financiera).
- Los logos de marca y aceptación en la parte derecha.
- El chip (si lo hubiese).
- El Personal Account Number (PAN), o número de tarjeta.
- La fecha de caducidad de la tarjeta.
- El nombre del titular.

En el reverso de la tarjeta figurará:

- La banda magnética: contiene grabados los datos del titular y caracteres alfanuméricos que hacen que los cajeros y terminales actúen de una forma determinada.
- El panel de firmas.
- (Anton A. & Branden R., 2012)Carácter especial CVV (número de seguridad)
- Firma. (Council, 2008)

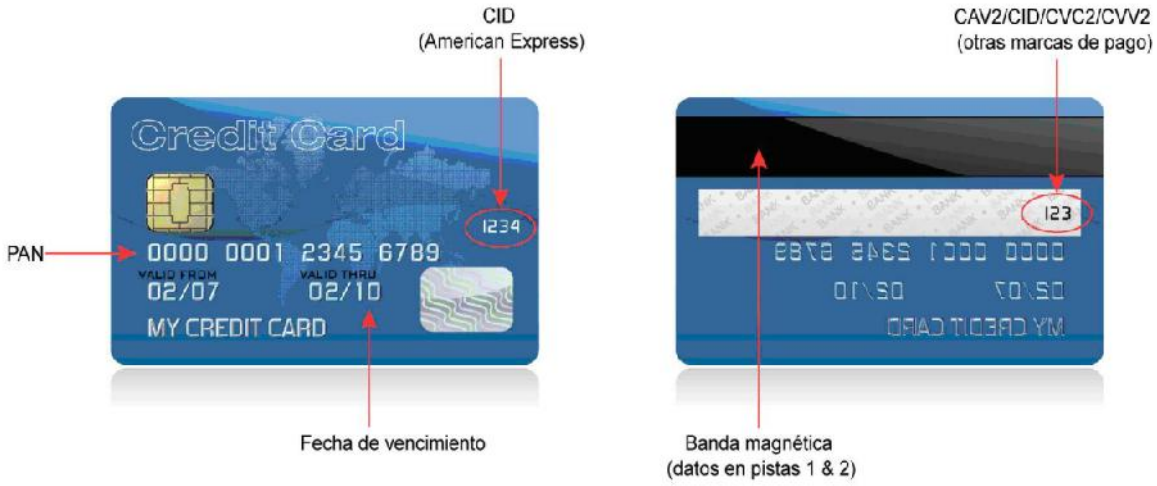


Ilustración 5 Componentes de la Tarjeta de Crédito

Fuente: Normas de la Seguridad de Datos de la Industria de Tarjetas de Pago

2.3.1. Estructura del Número de la Tarjeta de Crédito

Los primeros siete dígitos de todas las tarjetas se corresponden con el número de emisor de la empresa o entidad financiera y el país. Se incluye el primer número como parte del emisor para el tipo de tarjeta que hemos visto anteriormente. Por motivos de seguridad, los rangos completos de emisores y países son privados, aunque si se conocen los principales rangos de comienzo de cada una de las tarjetas.

Por ejemplo, las tarjetas VISA comienzan todas por 4, si son del tipo VISA Electron tienen rangos comprendidos entre 4026, 417500, 4508, 4844, 4913, 4917; Mastercard tiene asignados los rangos entre 51 y 55 y las tarjetas Maestro numeraciones de comienzo que sean alguno de estas series 5018, 5020, 5038, 6304, 6759, 6761, 6763

Estos rangos complementados hasta los 7 primeros dígitos ubican el tipo de tarjeta, el tipo de emisor y la zona geográfica en la que se ha emitido la tarjeta.

Resto de números de la tarjeta, todos los siguientes números, son el código interno de la entidad para asociar la tarjeta al cliente y corresponden con sus

propios criterios de numeración. El número total de dígitos de una tarjeta es variable, pudiendo oscilar entre 13 y 18, aunque las tarjetas más habituales tienen 16 dígitos.

Las excepciones típicas son American Express que tiene 15 dígitos, Dinners Club que tiene entre 14 y 15 dígitos y a partir de 16 dígitos para el resto, con un máximo de 19.

La mayoría de las tarjetas, destinan uno de esos dígitos al dígito de control. Este dígito es un número que cumple el algoritmo de Luhn, algoritmo que relaciona algebraicamente el resto de números para devolver el valor del dígito de control y se encuentra en una posición determinada. Para las tarjetas, VISA, Maestro y Mastercard, el dígito de control se encuentra en la posición 16.

No obstante, no todas las tarjetas tienen un dígito de control asociado. Por ejemplo algunos tipos de tarjetas Dinners Club no tienen este elemento de seguridad o las tarjetas emitidas por China mobipay no siguen el algoritmo de Luhn antes descrito.

Para motivos del proyecto se ha investigado los diferentes números de bines de las tarjetas de crédito de las diferentes instituciones a nivel del país, las cuales se encuentran en el **Anexo 1**

2.3.2. Funciones Básicas del tratamiento de la Información de Tarjetas de Crédito

Dentro de la complejidad general de las transacciones con tarjetas de crédito, las funciones realizadas dentro de cada subsistema tienden a ser conceptualmente claras. Así los datos entran en el sistema y luego son transmitidos, manipulados y presentados.

- Ingreso de datos.- Los datos entran al sistema de información en forma de transacciones que describen sucesos.

- Transmisión de datos.- Actualmente la transmisión de datos se la realiza por medio de sistemas informáticos distribuidos en los que los ordenadores a través de la organización están conectados por medio de una red de telecomunicaciones. Cada ordenados remoto sobre la red tiene, generalmente, capacidades de cálculo autónomo significativas para servir a las necesidades especializadas de sus usuarios locales proporcionando también acceso a los recursos mantenidos en otras localizaciones, eventualmente en un servidor con una potencia de procesamiento considerable y gran capacidad de almacenamiento en línea sobre disco. Los recursos necesarios no disponibles sobre un terminal de trabajo personal (estación de trabajo) pueden ser alcanzados a través de la red a nivel corporativo si se trata de recursos demasiado costosos para estar duplicados a nivel departamental. Es así que la red de telecomunicaciones tiene una combinación específica de topología de red, ancho de banda, con protocolo de comunicación, equipo terminal y proveedor de comunicaciones.
- Almacenamiento de datos.- El sistema de información debe mantener grandes ficheros de datos destinados a suministrar la información para el tratamiento de transacciones y para la toma de decisiones. Los principales aspectos que se consideran son la base de datos y la organización de los mismos en dicho sistema.
- Cálculo.- La forma habitual de cálculo implícita en la mayoría de los sistemas de información, se refiere a cálculos matemáticos, manipulación de datos y ejecución de diversas acciones de acuerdo con los resultados obtenidos. Mediante los cálculos el sistema de información transforma los datos brutos en información utilizable por el propio sistema o de forma ajena al mismo.
- Presentación de la información.- La función de presentación de un sistema de información proporciona una conexión esencial, o interfaz, entre el sistema y el usuario. Su finalidad es presentar la información de tal modo que mejore la capacidad del usuario para percibir y actuar sobre los hechos reflejados por la información.

Es así que para la aplicación de la Norma PCI-DSS el número de la tarjeta o PAN es el factor que define la aplicabilidad de los requisitos de las PCI-DSS, si no se almacena, procesa ni transmite no se aplicaran las normas PCI-DSS

2.4. Informática Forense

2.4.1. Análisis Forense

En informática forense se habla ya no sólo de recuperación de información sino de descubrimiento de información dado que no hubo necesariamente una falla del dispositivo ni un error humano sino una actividad encubierta para borrar, adulterar, ocultar o capturar información para acciones delictivas fraudulentas. Es por lo tanto esperable que el mismo hecho pase por desapercibido.

De tal manera previamente definiendo que es el análisis forense el cual se encarga de analizar sistemas informáticos en busca de evidencias mediante la aplicación de técnicas y herramientas de hardware y software para determinar datos potenciales o relevantes dentro de una exploración.

2.4.2. Metodología del Análisis Forense

Un proceso forense informático sigue una metodología particular y específica, que generalmente se divide en 4 fases tal como se indica en la Ilustración 6:

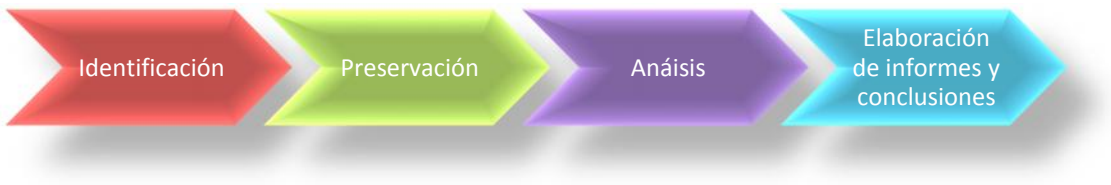


Ilustración 6 Fases del Proceso Forense Informático

1. Identificación (comprensión de la situación o circunstancias). Como un primer paso, al inicio de la investigación forense, se realiza un análisis. Se identifica información sobre un circunstancia en particular (puede ser de varias formas, mediante los sistemas de gestión de seguridad, mediante notificación directa, etc.), y hay una verificación de la misma, siendo importante probar las fuentes de información. Debe establecerse una línea de tiempo del evento y es importante saber lo que pasó en el momento de la adquisición de las pruebas. El escenario y sus circunstancias que se deben generar.

2. Reunión de pruebas En una segunda fase, se recogen las pruebas digitales. Normalmente, se une la evidencia digital a la información recuperada de un ordenador, pero este concepto va mucho más allá de esta asociación. Evidencias digitales son todo tipo de dispositivos que contienen información digital. Como con cualquier tipo de investigación, es necesario proporcionar evidencias para demostrar lo que queremos.

   Para un caso de investigación informática forense, es importante garantizar la fiabilidad y la integridad de la evidencia digital, por lo que es fundamental saber cómo manejarlas. Para que una evidencia digital sea válida, es necesario demostrar que esta es válida y que no ha sido manipulada anteriormente, porque los resultados de un caso dependerán en gran medida de la evidencia.

3. Análisis de pruebas En una tercera fase, para el análisis de evidencias digitales, hay algunos procedimientos a seguir que dependen, en gran medida, del tipo de escenario que fue diseñado antes, o del tipo de evidencia que se solicita. Algunos de los análisis que se pueden realizar son:

   - Definición de una línea de tiempo; -Análisis de palabras clave
   - Análisis de los encabezados de los archivos

- Análisis de los valores hash
- Análisis de la información oculta o borrada
- Análisis de Malware (por ejemplo, rootkits, troyanos, spyware, etc.)
- Análisis de los procesos
- Análisis de Registros
- Análisis del sistema de registro
- Esteganografía
- Análisis de correo electrónico
- Análisis de páginas web
- Análisis de la modificación de la información;
- Entre otros

4. Elaboración de informes y conclusiones Por último, se elaboran los informes con los resultados de los análisis realizados. A fin de explicar, de la mejor manera posible, las pruebas obtenidas, y así apoyar el proceso de resolución.

2.4.3. Análisis Forense en Redes

La forensia en redes de computo se trata de monitoreo de redes, determinando si existe alguna anomalía (o actividades maliciosas) y determinar la naturaleza de los ataques si dio alguno, dentro de los aspectos importantes incluye captura de tráfico, preservación y análisis. (Gomez, n/a, pág. 3).

La forensia en Red o Network Forensics es un escenario complejo, pues es necesario comprender la manera de como los equipos, protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento en particular. Entendiendo el funcionamiento de las redes de cómputo, se puede establecer los rastros, los movimientos y acciones. El contexto de forense en redes de cómputo exige capacidad de correlación de eventos, muchas veces separados y aleatorios.

Los datos de interés se pueden encontrar en muchos lugares, pero los más comunes en una red de datos pueden ser:

- Registros de los cortafuegos, Aplicación de Firewalls, de los IPS (sistemas de intrusión prevención) y de los IDS (sistemas de intrusión detección).
- Los protocolos de transferencia de hipertexto HTTP y el seguro HTTPS.
- En el protocolo de transferencias de archivos FTP.
- En los protocolos de los correos electrónicos. (SMTP, IMAP, POP y sus variantes).
- Cualquier otro protocolo que pudiera ser de interés, como por ejemplo SSH, LDAP, Telnet, etc.
- Conexiones lógicas del TCP/IP. IPv4, IPv6 de acuerdo a la Ilustración 7.
- Sistemas de enrutamiento, tablas ARP, respuestas a los escaneos de puertos y mensajes dados por el SNMP.
- Otra información que podamos encontrar del análisis del tráfico de red capturado por un sniffer.
- Sistemas de log centralizados, sistemas de correlación automatizada de eventos y soluciones UTM.
- Logs de aplicaciones de red. (Por ejemplo los logs de un servidor Apache o de un Internet Information Services IIS).
- Logs de plataformas virtuales. (VMware).
- Cualquier otra solución de seguridad empresarial que esté implantada y nos pueda ser de interés.

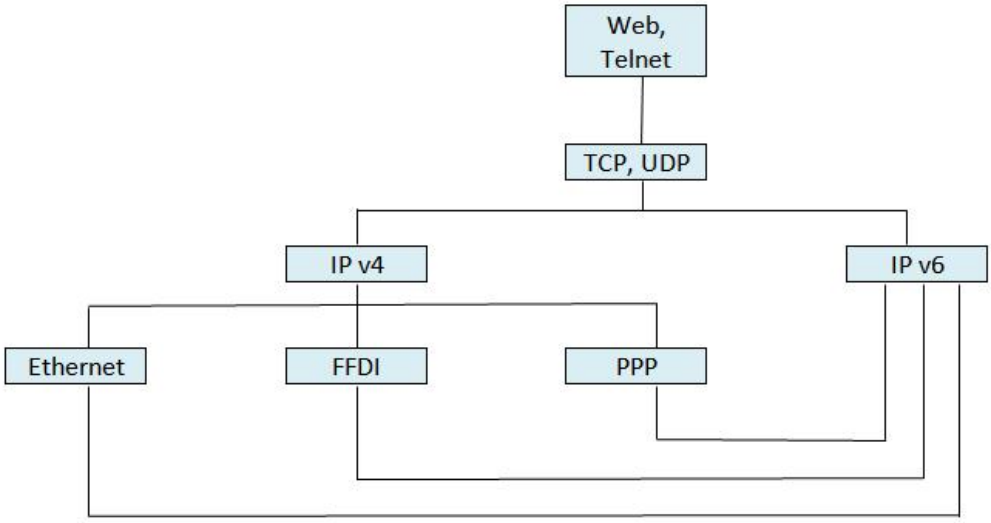


Ilustración 7 Conexiones Lógicas

Restos de tráfico de red que nos podemos encontrar en los discos duros, volcados de memoria RAM o de snapshots de máquinas virtuales. (Blog Profesional, 2013).

Es así que hoy en día, está en boca de todos conceptos como la nube, la nube compartida, las plataformas virtuales, las aplicaciones virtuales, escritorios remotos, etc. Por ello, desde hace unos años atrás, se viene insistiendo en que, a parte de esas típicas evidencias mencionadas anteriormente, hay más dispositivos o lugares donde se pueden encontrar datos de interés como puede ser en routers, firewalls, switches, etc. Y en algunos casos la información obtenida en estos lugares será la única y determinante para los resultados de una investigación.

Para obtener la citada información de estos dispositivos, se las debe realizar en tiempo real, en vivo o en caliente. Por ello, últimamente en la comunidad forense, se ha convertido en una prioridad que los profesionales, tanto del sector público como del privado, posean un amplio conocimiento de todo lo relacionado con la red. En concreto de cómo identificar, obtener, analizar e interpretar, en tiempo real el tráfico de datos que está circulando en una red, llámese lan, man o wan.

De tal manera que al Análisis forense de redes se la puede definir como una técnica de investigación de datos capturados a través del tráfico de red generado por un sistema. En el caso más simple el tráfico representa comunicación de la red conmutada por una de las partes durante el curso de alguna actividad, permitiéndonos hacer determinaciones forenses basadas en el tráfico de la red observada, que pueden ser relevantes en el curso de una investigación.

Teniendo en cuenta el análisis de red mediante un contexto forense se entenderá los eventos de la información observada en la captura de las tramas de red. Con el objetivo de realizar un análisis exhaustivo para establecer los hechos de alto nivel, como la atribución, la intención, la identidad, líneas de tiempo y otra información que pueden ser relevantes para la investigación de un determinado hecho.

El análisis de datos de una red es totalmente diferente a un análisis que se pueda hacer, por ejemplo, a un disco duro. Y es debido básicamente al espacio temporal de la información de la red. Cuando un ordenador está apagado, los datos de su disco duro permanecen intactos y estáticos (pueden darse excepciones como con los discos SSD). Pero en una red todo está en constante movimiento. En cualquier análisis de red en vivo, podríamos capturar el instante de la actividad en un momento dado.

Es por eso que los objetivos del análisis forense de redes son logrados de varias formas, pero la principal es la recolección y análisis de la evidencia digital.

Así pues desde el punto de vista forense, es más importante las deducciones de alto nivel que la información de un protocolo de red que se convertiría en algo de bajo nivel. Por ejemplo, en un típico caso de fraude que podría estar interesados en un archivo con información de interés que se ha enviado desde una computadora en la red. Nosotros al realizar el análisis forense tal vez estaríamos menos interesados, en la forma en cómo se envió el archivo (por ejemplo, utilizando el correo electrónico, la Web, páginas o mensajería instantánea), pero si

en el contenido del archivo en sí lo cual se convertiría en deducciones de alto nivel.

Por otra parte, queremos aplicar las técnicas y herramientas para realizar una búsqueda por palabras clave en el tráfico de red. Este enfoque es típico en análisis forense digital como una forma de controlar y regular las grandes cantidades de datos actuales.

Independientemente de los sistemas que se pueda encontrar a la hora de acudir a una inspección ocular digital (o respuesta a incidentes), debemos ser conscientes de que no sabemos cómo se encuentra la red, y que ello puede ocasionar problemas para adquirir información a través de la misma. Cualquier actividad podría influir o afectar a los datos recogidos. La red puede estar gobernada por un atacante y nos podemos topar con multitud de dificultades, como por ejemplo:

- Problemas con la retransmisión del TCP
- Existencia de servidores proxy
- El uso de correo electrónico
- Enrutamientos incorrectos
- Direcciones IP y/o de correo electrónico spoofeadas
- Ataques de man in the middle
- Secuestro de sesión TCP
- Envenenamiento de DNS

2.4.4. Fases de Análisis Forense en Red

Las fases principales de una metodología dentro del análisis forense en redes son las siguientes:

- Recolección del tráfico de la red
- Examinar y analizar del tráfico de la red
- Recomendaciones

Dentro de distintas bibliografías consultadas referentes a la aportación de información en el análisis forense se han encontrado puntos en común que se toman como base para plantear las fases de una metodología de análisis forense en redes. Tales fases se muestran en la Ilustración 8 y son las siguientes:

- Identificación del incidente
- Recolección y Preservación de la evidencia
- Evaluación de los datos
- Análisis de la información
- Reporte de resultados.

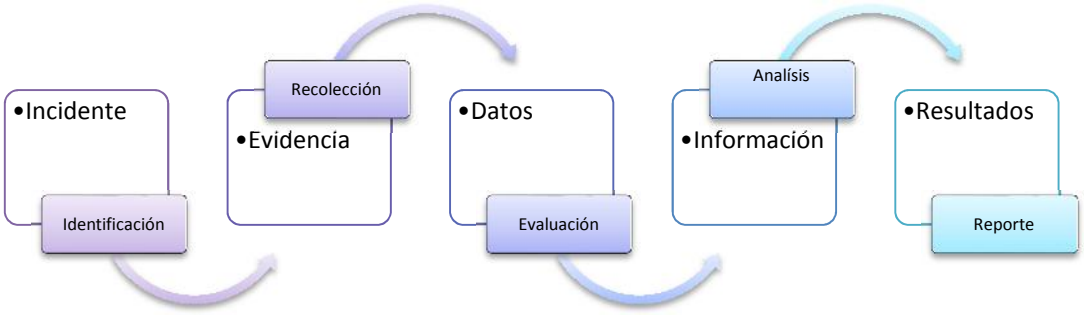


Ilustración 8 Metodología Análisis Forense

2.4.5. Fases de un ataque informático

Los ataques contra redes y sistemas informáticos tienen distintas fases o etapas, algunas de ellas se presentan continuación:

- Descubrimiento y explotación del sistema informático.
- Búsqueda e identificación de vulnerabilidades en el sistema.
- Explotación de las vulnerabilidades detectadas (para ello, se utilizan herramientas específicamente construidas para tal fin, por ejemplo exploits)
- Compromiso del sistema: Es la modificación de programas y archivos del sistema para dejar instaladas determinadas puertas traseras o troyanos;

creación de nuevas cuentas con privilegios administrativos que faciliten el posterior acceso del ataque al sistema afectado

- Eliminación de las pruebas que pueden revelar el ataque y el nivel de compromiso del sistema: Se basa en la eliminación o modificación de los registros de actividad del equipo “logs”; modificación de los programas que se encargan del monitoreo de la actividad del sistema.

2.5. Herramientas de ataques en redes

En cuanto a los medios y herramientas disponibles en la actualidad para realizar ataques en redes de cómputo existen las siguientes:

- ***Scaneo de puertos***: que permiten detectar los servicios instalados y puertos abiertos en un determinado sistema informático
- ***Sniffers:*** dispositivos que capturan los paquetes de datos que circulan por una red
- ***Exploits:*** herramienta que busca y explota vulnerabilidades conocidas
- ***Backdoors kits:*** programas que permiten explorar y abrir puertas traseras en los sistemas
- ***Rootkits:*** programa utilizado para ocultar puertas traseras en los propios archivos ejecutables y servicios del sistema, que son modificados para facilitar el acceso y posteriormente controlar el sistema
- ***Auto - rooters:*** herramientas capaces de automatizar totalmente un ataque, escanear sus posibles vulnerabilidades, explotarlas y obtener acceso al sistema comprometido
- ***Password crackers:*** aplicaciones que permiten averiguar las contraseñas de los usuarios de sistemas comprometidos
- ***Analizador de vulnerabilidades:*** herramienta que analiza al equipo en búsqueda de fallos de seguridad
- ***Técnicas de spoofing:*** facilitan la ocultación y la suplantación de direcciones IP, dificultando en este modo la identificación del atacante.

2.6. Recolección de Información de la Red

Generalmente el primer paso es saber de qué forma se debe recolectar la información y qué tipo de información será necesaria. La meta es recolectar la información acerca de los servidores residentes y construir una base de datos que contenga la estructura de red de la organización.

De los protocolos y herramientas para la recolección de información de la red se pueden mencionar las siguientes:

- El programa TraceRoute puede revelar el número de redes intermedias y los ruteadores en torno a un servidor específico.
- El comando Whois se basa en el uso del Protocolo TCP (Protocolo de Control de Transmisión) basado en petición/repuesta que se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IPen Internet.
- El Programa Nslookup realiza consultas al DNS (Servidor de Nombres de Dominio) para obtener una lista de las direcciones IP y sus correspondientes nombres.
- El protocolo Finger puede revelar información detallada acerca de los usuarios (nombres de Login, números telefónicos, fecha y hora de última sesión, etc.) de un equipo en específico.
- El protocolo SNMP (Protocolo Simple de Administración de Red) se utiliza para examinar la tabla de ruteo de un dispositivo, esto es útil para conocer los detalles de la topología de red perteneciente a una organización.
- El protocolo ICMP (Protocolo de Control de Mensajes de Internet) se emplea para localizar un equipo en particular y determinar si se puede alcanzar desde un segmento de red. Este protocolo es usado por el comando ping que realiza un escaneo por medio de llamadas a la dirección de un servidor haciendo posible construir una lista de los servidores que actualmente pertenecen a la red.

2.7. Escaneo de Vulnerabilidades

Un escaneo de vulnerabilidades se utiliza para probar el nivel de seguridad en un equipo determinado dentro de una red; un administrador de redes hábil puede usar estas herramientas en su red privada para descubrir los puntos potenciales donde es vulnerable su seguridad y así, determina que equipos necesitan ser actualizados, pero los atacantes utilizan los resultados obtenidos para intentar un acceso no autorizado.

A continuación se presentan algunos usos de las herramientas que funcionan de manera automática y que son utilizadas con mayor frecuencia por los atacantes para explorar individualmente los servicios proporcionados por una red de cómputo:

- Varias herramientas son de dominio público, tal es el caso de ISS (Internet Security Scanner) o la herramienta de Análisis de Seguridad para Auditoria de Redes (SATAN), la cual puede rastrear una subred o un dominio y ver las posibles fugas de seguridad. Estos programas determinan la debilidad de cada uno de los sistemas
- Una vez obtenida una lista de las vulnerabilidades de los servicios en la red, se puede escribir un pequeño programa que intente conectarse a un puerto especificando el tipo de servicio que está asignado al servidor en cuestión. La aplicación del programa presenta una lista de los servidores que soportan servicio de Internet y están expuestos al ataque.

Después de lograr el acceso a un sistema protegido, se presentan una infinidad de opciones con las cuales el atacante podrá causa daño, estas opciones pueden ser las siguientes:

- Se puede atentar destruyendo toda evidencia del ataque y además seguir teniendo acceso sin que el ataque original sea descubierto
- Pueden instalar paquetes que incluyan códigos binarios conocidos como "caballos de Troya" protegiendo su actividad haciéndola transparente. Los paquetes recolectan las cuentas y contraseñas para los servicios de Telnet y

FTP (Protocolo de transferencia de archivos) permitiendo expandir su ataque a otras máquinas

- Se puede obtener acceso privilegiado a un sistema compartido

CAPITULO III

3.1. Normativa y Aspectos Técnicos

3.1.1. PCI-DSS

La seguridad de la información de titulares de tarjetas se ha convertido en una verdadera preocupación en todo el mundo, tanto para los bancos que emiten de tarjetas de pago como para los comercios que las aceptan y por supuesto, para los clientes que las utilizan.

En muchos países, se han producido casos en los cuales delincuentes acceden a sistemas informáticos, roban la información de tarjetas y utilizan estos datos para cometer fraudes. En la mayoría de los casos, estos sistemas informáticos han sido operados por comercios que aceptan tarjetas de pago o por vendedores que procesan pagos en su nombre. Como respuesta a este problema, Visa ha desarrollado las Normas de Seguridad de la Información de la Industria de Medios de Pago (PCI DSS) en colaboración con MasterCard. Se trata de un conjunto de exigencias y procesos comunes a todo el sector respaldado por todos los principales sistemas internacionales de tarjetas de pago.

Como es conocido, PCI-DSS impone que entre los datos de los titulares de las tarjetas, el número de tarjeta o PAN, que se permite almacenar, sea ilegible (requerimiento 3.4) que en particular requiere lo siguiente:

3. Proteger los datos del titular de la tarjeta
    - 3.2. No registrar los datos sensibles después de la autorización (aunque los datos sean encriptados).
    - 3.3. Enmascarar el PAN cuando se presenta en las pantallas.
    - 3.4. Hacer el PAN inteligible en todos los lugares donde se registra.

Tabla 2 Datos Tarjeta de Crédito

Los datos de titulares de tarjeta incluyen	Los datos confidenciales de autenticación incluyen
• **Número de cuenta principal (PAN)** • **Nombre del titular de la tarjeta** • **Fecha de vencimiento** • **Código de servicio**	• Todos los datos de la banda magnética o datos equivalentes que están en un chip • PIN / Bloqueos de Pin

Los requisitos de las PCI DSS se aplican a todos los componentes del sistema que se incluyen en el entorno de los datos del titular de la tarjeta o que están relacionados con éste. El entorno de los datos del titular de la tarjeta es la parte de la red que posee los datos del titular de la tarjeta o los datos confidenciales de autenticación, incluidos los componentes de la red, los servidores y las aplicaciones.

- Los componentes de la red incluyen, a modo de ejemplo, firewalls, interruptores, routers, puntos de acceso inalámbricos, dispositivos de red y otros dispositivos de seguridad.
- Los tipos de servidores incluyen, a modo de ejemplo: web, base de datos, autenticación, correo electrónico, proxy, protocolo de tiempo de red (NTP) y servidor de nombre de dominio (DNS).
- Las aplicaciones incluyen todas las aplicaciones compradas y personalizadas, incluidas las aplicaciones internas y externas (Internet).

Metodológicamente el proceso de implementación de PCI-DSS puede asumirse a través del siguiente Ciclo de Deming para el mejoramiento continuo como se muestra en la Ilustración 9.

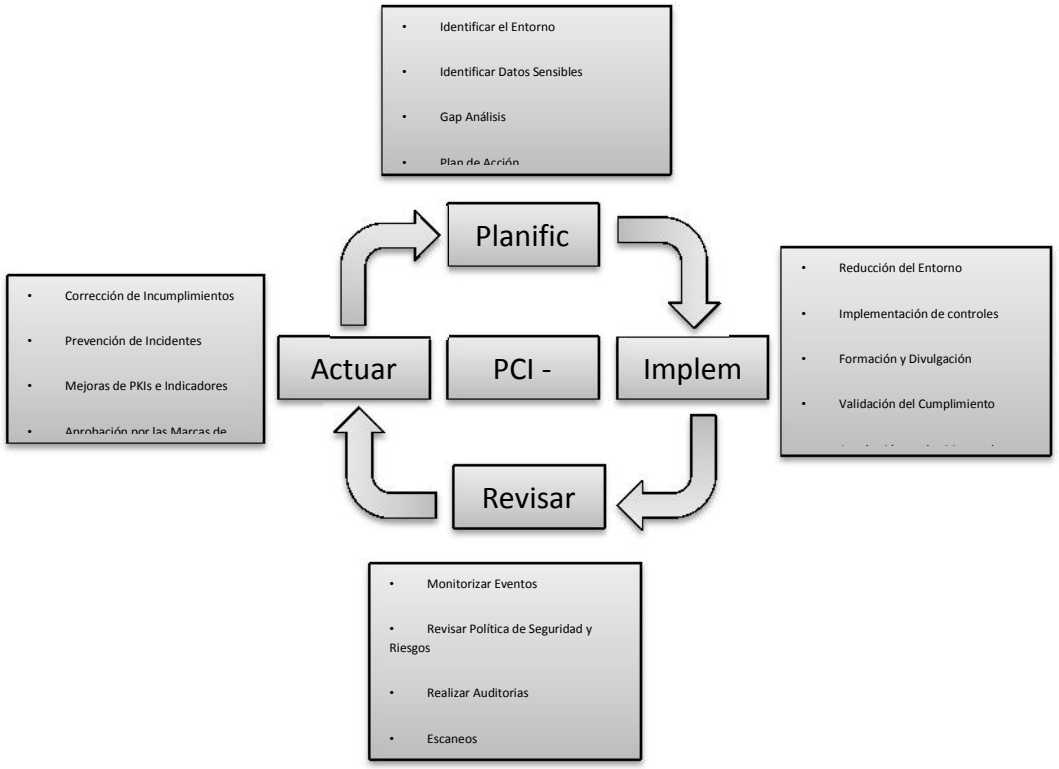


Ilustración 9 Ciclo Deming

Para efectos de auditoria y evaluación de PCI – DSS homologa empresas como Qualified Security Assessors (QSA), que son personas encargadas de realizar una revisión del sistema y reportar al ente solicitante los resultados del análisis y Approved Scan Vendor (ASV); que son empresas dedicadas a realizar escaneos de seguridad externos. Dependiendo del nivel de transacciones con tarjetas de crédito que la organización realice anualmente, se deben realizar escaneos de seguridad trimestrales por un ASV, estar sujetos a auditorias anuales por parte de un QSA o diligenciar un Self-Assessment Questionnaire (SAQ) (PCI QSA y ASV, 2009), para garantizar que los controles se encuentran satisfactoriamente desplegados y son monitoreados de forma continua.

PCI-DSS fue creado para proteger la confidencialidad, integridad y disponibilidad de los datos relacionados con tarjetas de pago. De allí, la importancia en contar con una buena gestión de eventos y registros que permitan

prevenir, detectar, contener, corregir y evaluar cualquier amenaza que afecte a dicha información y soporte cualquier proceso investigativo y/o actividad legal posterior a un incidente.

En este sentido existe dentro de la especificación el Requisito 10: “Rastrear y monitorizar todo el acceso a los recursos de la red y datos de los tarjetas habientes”, orientado hacia la definición de mecanismos de registro y a su gestión. Además del Requisito 11: “Pruebe regularmente los sistemas y procesos de seguridad” la cual está orientada a realizar pruebas de sistemas, procesos y software con frecuencia para asegurar que la seguridad se mantenga con el tiempo y con algunos cambios en el software.

3.1.2. Requisito 10 Norma PCI-DSS

3.1.2.1. Requisito 10: “Rastrear y monitorizar todo el acceso a los recursos de la red y datos de los tarjetas habientes”

En este requisito se determina los lineamientos y procesos de auditoria que garanticen que se cuenta con los siguientes controles definidos, implementados y en ejecución:

Procesos de vinculación de todos los accesos de cada usuario a los componentes del sistema: mediante este control se pretende garantizar que cada acceso al sistema, corresponde a un usuario plenamente identificable y rastreable, especialmente aquellos de tipo administrativo. Obviamente, este control depende de que anteriormente se haya ejecutado una labor de asignación de cuentas particulares a cada usuario, eliminando las cuentas grupales y estableciendo los controles sobre cuentas por defecto, controles contemplados en el Requisito 7 y 8 del estándar.

3.1.2.2. Implementación de pistas de auditoria automatizadas para todos los componentes del sistema

La determinación de la causa de un incidente es muy difícil, si no se cuenta con registros de la actividad realizada sobre el sistema. Por ello, es necesario garantizar la existencia de un registro de todos los accesos al sistema, todas las acciones de tipo administrativo realizadas por cuentas interactivas, cualquier acceso a los registros de auditoría y creación y eliminación de objetos a nivel del sistema.

3.1.2.3. Elementos a ser registrados en las pistas de auditoria

Con el propósito de certificar que los registros de auditoría cuentan con la suficiente información para tener trazabilidad completa, se requiere que los siguientes elementos estén presentes en cada entrada: identificación del usuario, tipo de evento e información acerca de los datos, componentes o recursos afectados por la acción ejecutada.

3.1.2.4. Sincronización de relojes y horarios en el sistema

Con el fin de poder correlacionar en forma satisfactoria los eventos generados por cada componente del sistema, independientemente de su ubicación, se requiere que exista un elemento de sincronización central. Para ello, se recomienda implementar NTP (Network Time Protocol) o tecnologías similares, definir uno o varios servidores que se sincronicen con elementos externos y confiables y distribuyan internamente dicha sincronización, empleando de formas opcionales cifradas y listas de control de acceso (ACL) con estos hosts.

3.1.2.5. Resguardo y protección de los registros de auditoria

Para prevenir que los registros de auditoría sean modificados y garantizar su integridad, inclusive bajo los privilegios del administrador del sistema, se deben

implementar controles orientados hacia la separación de los roles y la necesidad de saber. Para ello, se debe limitar la visualización de los registros de auditoria únicamente a aquel personal que por consideraciones operativas o administrativas lo requiera, aplicar controles para proteger la integridad de dichos registros, emplear un servidor central de registros como repositorio de datos relacionados con eventos de servidores, aplicaciones, bases de datos, equipos activos de red y de seguridad perimetral. De igual manera, es importante emplear un software de monitorización de integridad de archivos, que permita identificar cualquier cambio realizado sobre los registros de eventos.

Revisión de los registros de eventos de los componentes por lo menos una vez al día

La clave de los registros de eventos está en su revisión. Es un esfuerzo vano definir una arquitectura robusta de monitoreo, si no se ejecutan acciones sobre las alertas generadas. Para esto, PCI-DSS requiere que los registros de eventos sean revisados por lo menos una vez al día y es precisamente en este punto donde las herramientas de centralización y generación de reportes automatizadas entran en acción.

3.1.2.6. Conservar los registros de auditoria

Finalmente para el cumplimiento de PCI-DSS es necesario que los registros de auditoria sean almacenados como mínimo durante un año, con disponibilidad inmediata de por lo menos los últimos tres meses para análisis.

El enfoque metodológico a aplicar en el análisis forense basado en la norma PCI-DSS tiene un enfoque orientado a la mejora continua de la seguridad de los sistemas afectados, orientando a la Universidad Tecnológica Equinoccial a mantener y aumentar la seguridad de forma global.

De forma general el análisis forense se desarrollara en cuatro fases de acuerdo a la Ilustración 10, que tienen como principales objetivos delimitar el entorno afectado, identificar los puntos de no conformidad con la norma y orientar en las acciones que deban tomarse para subsanarlos, hasta la emisión del informe del cumplimiento final.

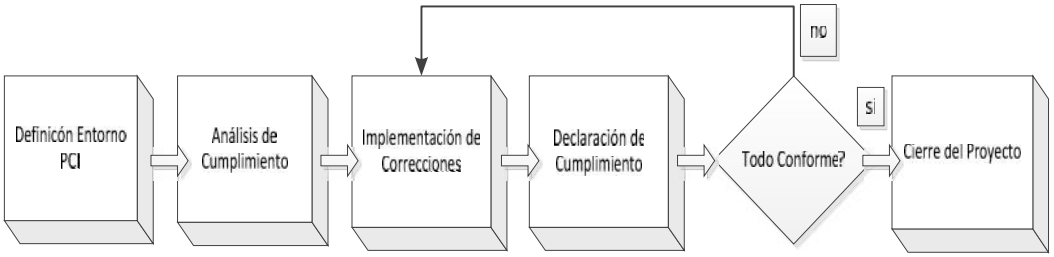


Ilustración 10 Implementación PCI

Debido al coste que se supone la implementación de los requisitos de la norma PCI-DSS, en la primera fase del proyecto cobra especial importancia la delimitación del alcance y la identificación de los componentes afectados. En muchas ocasiones, es posible reducir el coste y esfuerzo utilizando una adecuada segmentación de red eliminando datos innecesarios, aislando sistemas, etc. Es por ello que dentro de esta tesis se dedicó un esfuerzo necesario en esta primera fase con objeto de simplificar el posterior proceso de cumplimiento.

Durante la fase de análisis, utilizamos los procedimientos de prueba y criterios de evaluación definidos por PCI-DSS, ya que de esta forma es posible garantizar el cumplimiento de los requisitos frente a quienes después exigirán los informes de auditoría (entidades adquirientes, comercios o las propias compañías de tarjetas). Identificamos no solo los puntos de conformidad, sino también las oportunidades de mejora y recomendaciones para el cumplimiento de PCI-DSS.

Finalmente se presentará un Informe de Cumplimiento y Declaración de Cumplimiento además se incluirá las no conformidades, para que la universidad pueda resolver esos inconvenientes detectados dentro del análisis.

3.1.3. Requisito 11 Norma PCI-DSS

3.1.3.1. Probar regularmente los sistemas y procesos de seguridad

Por medio de este requisito lo que se trata es de que los delincuentes que roban datos de los computadores no ingresen a los sistemas de la Universidad exactamente en las áreas donde se manejan los pagos a través de la tarjetas de crédito y a los equipos donde se está guardando su información confidencial de cada dueño de la tarjeta, pero continuamente se está descubriendo nuevos ataques que se introducen por medio de software nuevos. Los sistemas, procesos y programas deben estar frecuentemente probándose para garantizar que se mantengan su seguridad a través del tiempo y cambios.

3.1.3.2. Vulnerabilidades de la Red

Como parte de la auditoria dentro de la Universidad Tecnológica Equinoccial y básicamente basándose en la norma PCI-DSS se debe realizar lo siguiente:

Se debe revisar tanto internos y externos las vulnerabilidades de red al menos trimestralmente y después de cada cambio significativo en la red (tales como instalaciones de componentes del sistema, cambios en la topología de red, modificaciones en las normas de firewall, actualizaciones de productos), es decir se debe contar con un procedimiento para detectar nuevas vulnerabilidades, principalmente consultando fuentes externas que ayuden a la Universidad.

Como parte del procedimiento se deben verificar lo siguiente:

- Verificar que se realicen análisis de vulnerabilidad externa e interna de la siguiente manera:
    - Revisar los informes de los análisis y verifique que se hayan realizado cuatro análisis internos trimestrales durante el período de 12 meses más reciente.

- Revisar los informes de los análisis y verifique que el proceso de análisis incluya la repetición de los análisis hasta que se obtengan resultados de aprobación o hasta que se resuelvan todas las vulnerabilidades.
- Verificar que la prueba se haya realizado con un recurso interno calificado o bien que la haya realizado un tercero capacitado, y cuando corresponda, que la persona que realice la prueba sea independiente de la empresa.

- Realizar análisis de vulnerabilidad interna trimestralmente de la siguiente manera:
  - Revisar los informes de los análisis y verifique que se hayan realizado cuatro análisis internos trimestrales durante el período
  - Revisar los informes de los análisis y verifique que el proceso de análisis incluya la repetición de los análisis hasta que se obtengan resultados de aprobación o hasta que se resuelvan todas las vulnerabilidades
  - Verificar que la prueba se haya realizado con un recurso interno calificado o bien que la haya realizado un tercero capacitado, y cuando corresponda, que la persona que realice la prueba sea independiente de la empresa
- Los análisis trimestrales de vulnerabilidades externas debe realizarlos un Proveedor Aprobado de Escaneo (ASV) certificado por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC)
- Realice análisis internos y externos después de cualquier cambio significativo.

3.1.3.3. Sistemas de Detección de Intromisión

Utilizar los sistemas de detección y/o prevención de intrusiones para supervisar el tráfico en el perímetro del entorno de datos de titulares de tarjetas,

así como los puntos críticos dentro del entorno de datos de titulares de tarjetas y alerte al personal ante la sospecha de riesgos.

Mantenga actualizados todos los motores, líneas base y firmas de detección y prevención de intrusiones.

- Verifique el uso de los sistemas de detección y/o prevención de intrusiones y que todo el tráfico en el perímetro del entorno de datos de titulares de tarjetas, así como los puntos críticos dentro del entorno de datos de titulares esté supervisado
- Confirme que estén configurados el IDS y/o IPS para alertar al personal ante la sospecha de riesgos
- Examine la configuración de IDS/IPS y confirme que los dispositivos de IDS/IPS estén configurados, se mantengan y se actualicen según las instrucciones del proveedor para garantizar una protección óptima.

3.2. Análisis de Herramientas

3.2.1. Sniffer

Sniff es un vocablo que proviene de la lengua inglesa y podemos traducir al castellano como husmear. Y en la práctica el aplicar técnicas de sniffing lo que haremos es escuchar el tráfico de la red, se lo guardará para posteriormente analizarlos obteniendo información sobre nuestro objetivo el cual es información relacionada con tarjetas de crédito y tarjeta habientes.

Sin tener acceso a ningún sistema de la red, se puede obtener información, claves de acceso o incluso mensajes de correo electrónico en el que se envían estas claves.

La forma más habitual de sniffing, probablemente porque está al alcance de cualquiera, es la que podríamos llamar sniffing por software, utilizando un programa que captura la información de la red.

También es posible hacer lo que podríamos llamar sniffing hardware, que pasaría por conectar en un cable de red un dispositivo que permita capturar el tráfico.

Con relación a este último tipo, la expresión "conectar el cable de red" es una expresión general que incluye el propio hecho de conectar un dispositivo a un cable de la red pero también incluye, por ejemplo, un receptor de radio que se sitúa en medio de un radio enlace. Como se puede imaginar, este tipo de técnicas requiere de unos conocimientos de electrónica adicionales muy importantes. Lo que se trata en este capítulo es conocer sobre los sniffers software, ya que existe una gran cantidad de ellos y se podrá probarlos, detectarlos y eliminarlos dentro de un ambiente laboral

Como se indica en la Ilustración 11 la idea general de un sniffer es capturar todos los paquetes que pasan por delante de la PC en la que está instalado. Esto quiere decir que un sniffer no es un objeto mágico que una vez lanzado puede ver todo lo que sucede en la red. Dicho de otra forma, un usuario que se conecte a Internet vía módem e instale un sniffer en su máquina sólo podrá capturar los paquetes de información que salgan o lleguen a su máquina.

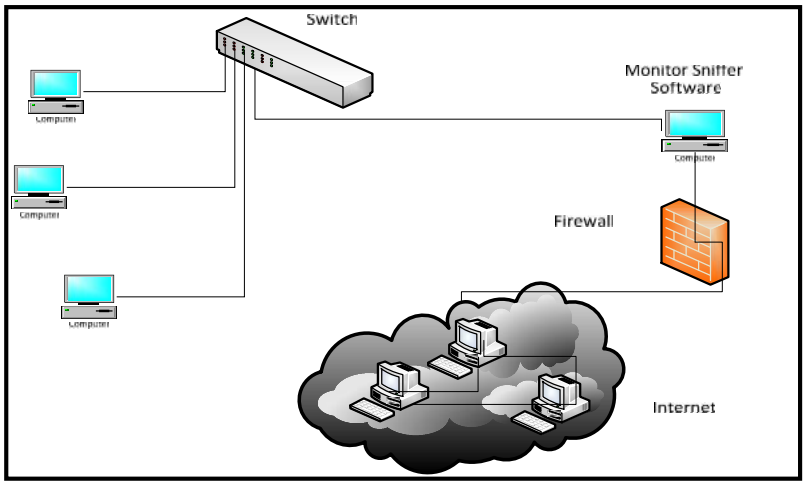


Ilustración 11 Funcionamiento de un Sniffer

El entorno en el que suele ser más efectivo este tipo de programas es en una Red de Área Local (LAN), montada con la topología tipo bus. En este tipo de redes todas las máquinas están conectadas a un mismo cable, que recibe el nombre de bus, y por lo tanto, todo el tráfico transmitido y recibido por todas las máquinas que pertenecen a esa red local pasa por ese cable compartido, lo que en la terminología de redes se conoce como el medio común. El Hub o concentrador opera igual que un cable bus.

El otro entorno natural de los sniffers es una máquina víctima. En este caso, es necesario tener acceso a la máquina victima para instalar el programa y el objetivo perseguido aquí es robar información que permita el acceso a otras máquinas, a las que habitualmente se accede desde esa máquina víctima.

Los sniffers funcionan por una sencilla razón: muchos de los protocolos de acceso remoto a las máquinas se transmiten las claves de acceso como texto plano, y por lo tanto, capturando la información que se transmite por la red se puede obtener este tipo de información y el acceso ilegítimo a una determinada máquina.

Uno de los entornos naturales para un sniffer es una LAN con topología de bus. Las redes más comunes de este tipo son las conocidas como buses Ethernet. Estas redes están formadas por una serie de computadoras, cada una de ellas equipada con una tarjeta de red Ethernet y conectadas a través de un Hub o concentrador.

Cada vez que una máquina de la LAN desea transmitir un dato lo hace a través del hub que están conectadas todas las máquinas, por lo que todas tienen la posibilidad de ver los datos que se están transmitiendo, aunque en condiciones normales esto no sucede.

Las tarjetas de red Ethernet están construidas de tal forma que, en su modo normal de operación, sólo capturan los paquetes de datos que van dirigidos hacia ellas, ignorando la información cuyo destino es otra máquina. Lo que esto

significa es que, en condiciones normales, el tráfico que circula por el hub no puede ser capturado y es necesario activar un modo especial de funcionamiento de la tarjeta conocido como modo promiscuo.

En este modo, la tarjeta de red captura todos los paquetes que pasan por el hub en el que está conectada y éste es el modo de operación que un sniffer necesita para llevar a cabo su finalidad.

Modo Promiscuo cuando la tarjeta o adaptador de red se configura en modo promiscuo, captura todos los paquetes que pasan por delante de él.

La forma más inmediata de saber si un determinado adaptador de red está en un modo promiscuo es utilizar el programa ifconfig. Este programa permite configurar los adaptadores de red instalado en una determinada máquina y obtener información de esa configuración.

Cuando un adaptador de red se encuentra en modo promiscuo, ifconfig nos informa de ello. Un intruso que rompa un sistema e instale un sniffer en él sustituirá este programa por una versión modificada, de tal forma que no muestre el estado en modo promiscuo de la interfaz de red.

El modo de funcionamiento promiscuo, podemos decir que en los kernel más modernos esta información puede ser obtenida a partir del sistema de ficheros /proc, lugar del que podemos obtener una enorme cantidad de información interesante sobre el sistema de red.

3.2.2. Captura de Paquetes

Como introducción a la seguridad informática y con el objetivo de visualizar los paquetes que circulan por la red, se realiza la captura de paquetes a través del (network sniffing).

Un sniffer es un programa de para monitorear y analizar el tráfico en una red de computadoras, detectando los cuellos de botellas y problemas que existan en ella, esta sería una definición de su uso “legal”, porque también podemos interceptar las comunicaciones de los programas de conversación (MSN, IAM, ICQ…) e incluso filtrar el tráfico http, POP, SMTP y ver claves, mensajes y demás.

El entorno en el que suele ser más efectivo este tipo de programas es en una Red de Área Local (LAN), montada con la topología tipo bus. En este tipo de redes todas las máquinas están conectadas a un mismo cable, que recibe el nombre de bus, y por lo tanto, todo el tráfico transmitido y recibido por todas las máquinas que pertenecen a esa red local pasa por ese cable compartido, lo que en la terminología de redes se conoce como el medio común.

Los sniffers suelen trabajar, de tal forma que no sólo capturan la información asociada a los protocolos de aplicación como FTP o TELNET, sino que capturan paquetes raw y, por lo tanto, toda la información contenida en las cabeceras TCP/IP.

Muchas de estas herramientas disponen de la capacidad de interpretar estas cabeceras, e incluso las cabeceras asociadas a protocolos que se encuentra por debajo de IP, y mostrarlas de forma más sencilla de interpretar para los seres humanos. Cuando los sniffers se utilizan de esta forma son llamados Analizadores de protocolo. Si bien, esta palabra designa a un gran conjunto de herramientas (algunas incluso hardware).

Es así que dentro del Ecuador se ha utilizado las técnicas del sniffer dentro de instituciones públicas como privadas, en donde tienen enlaces que conectan diferentes redes, estos enlaces pueden ser entre redes privadas a redes públicas (Internet). Como ejemplo se menciona que en Tungurahua “Dentro del Hospital Regional Docente Ambato (HRDA) que es una institución pública que ha incrementado en el uso de la tecnología y el acceso a una red de computadoras, el problema actual en el Departamento de Sistemas del HRDA se originan

fundamentalmente porque existe un desconocimiento de las falencias de los servidores WEB, MAIL y FTP ya que el flujo de información que circula a través de esta red es de alta importancia por lo que conocer algunos de los puntos débiles dentro de estos servidores sería de gran importancia, es así que a través del Sniffing se pudo detectar vulnerabilidades dentro de su red, lo cual ayudará para que se puedan tomar decisiones correctas con respecto al mejor manejo de los recursos de la red dentro de la institución" (UTA).

Dentro de las aplicaciones que realizan tareas de sniffing tenemos a:

Driftnet es un sniffer de imágenes, en combinación con un arp spoofer, podemos hacer que el tráfico de la red venga a nuestra interfaz, es otra alternativa a un ataque man in the middle, donde podemos analizar todo el tráfico de imágenes.

Dsniff es una colección de herramientas para auditar redes y hacer pruebas de penetración. Monitoriza la red para obtener datos importantes como contraseñas, direcciones de correo electrónico, archivos, etc.

Tcpdump es una herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red. Permite al usuario capturar y mostrar a tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado.

WireShark la misma que es de libre distribución y es un estándar de facto para la realización de esta tarea además de ser una de las aplicaciones más popular, de software libre y multiplataforma. Se suele emplear para redes Ethernet y WiFi. También existe la opción de realizar el análisis desde el propio terminal en redes WiFi y 3G con tPacketCapture.

De acuerdo a los análisis de las herramientas de sniffing descritos anteriormente se eligió a WireShark por las siguientes razones:

- Es software OpenSource,
- Existe versiones para Windows y Linux,
- Permite realizar filtrado de paquetes,
- Permite registrar el tráfico de la red en archivos,
- Maneja interfaz gráfica amigable,
- Maneja diferentes formatos *.pcap

3.2.1. Herramienta de Análisis de Redes WireShark

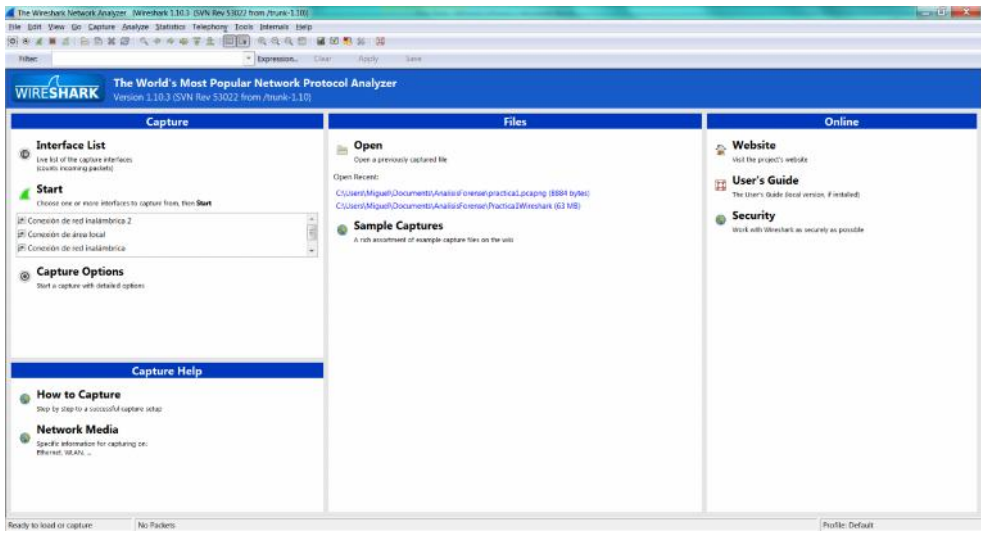


Ilustración 12 Interfaz WireShark

Fuente: Software WireShark

En el año 2006 se oficializó el nombre de WireShark que antes de esta fecha se conocía como Ethereal y hoy en día está catalogado como uno de los TOP 10 como sniffer junto a Nessus y Snort ocupando el segundo lugar entre estos.

Este sniffer o analizador de protocolo, es uno de los que ofrece una interfaz más sencilla de utilizar y permite visualizar los contenidos de las cabeceras de los protocolos involucrados en una comunicación de una forma muy cómoda.

Funciona en modo gráfico y está programado con la librería de controles GTK.

Características:

- Disponible para Unix, Linux, Windows y Mac OS.
- Captura los paquetes de datos de la red directamente desde una interfaz de red.
- Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.
- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Filtra y busca los paquetes que cumplan con un criterio definido previamente.
- Permite obtener estadísticas.
- Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos

WireShark no es un IDS (Instrusion Detection System), sin embargo permite analizar y solventar comportamientos anómalos en el tráfico de la red.

La ventana principal de la aplicación se divide en tres partes.

En la primera parte se muestra la información más relevante de los paquetes capturados, como, por ejemplo, las direcciones IP y puertos involucrados en la comunicación como se muestra en la Ilustración 13. Seleccionando un paquete en esta sección podemos obtener información detallada sobre él en las otras dos secciones de la pantalla que comentaremos a continuación.

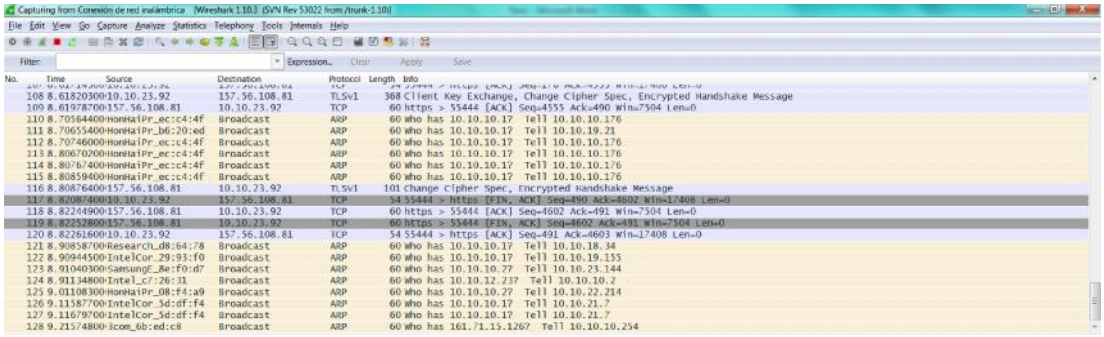


Ilustración 13 Paquetes Capturados - WireShark

Fuente: Software WireShark

En la parte central de la ventana se muestra, utilizando controles tree, cada uno de los campos de cada una de las cabeceras de los protocolos que ha utilizado el paquete para moverse de una máquina a la otra. Así, si hemos capturado una serie de paquetes de, por ejemplo, una conexión telnet, podremos ver las cabeceras del protocolo TCP, del IP y de los que tengamos debajo de ellos (Ethernet Frame, por ejemplo, en una red Ethernet).

Ilustración 14 Cabecera de Protocolos – WireShark

Fuente: Software WireShark

La tercera parte de la ventana muestra un volcado hexadecimal del contenido del paquete. Seleccionando cualquier campo en la parte central de la ventana se mostrarán en negrita los datos correspondientes del volcado hexadecimal, los datos reales que están viajando por la red.

Ilustración 15 Contenido del Paquete – WoreShark

Fuente: Software WireShark

Otra opción que ofrece este programa es la de seguimiento de flujos TCP (Follow TCP Stream). Esta opción permite, una vez seleccionado un paquete de entre los capturados, recuperar sólo los paquetes asociados a la misma conexión que el seleccionado. Esta opción es muy útil, ya que el sniffer captura todos los paquetes y si en un momento dado existen varias conexiones distintas los paquetes de todas ellas aparecerían entremezclados.

Lo que se debe recordar es que, tanto para activar el adaptador de red en modo promiscuo, como para crear sockets raw, el intruso debe ser root.

3.2.2. Función de Búsqueda de Paquetes

Cuando iniciamos la captura de paquetes por lo general se obtiene una gran cantidad de paquetes que cumple con los filtros y/0 expresiones definidas, WireShrak permite realizar búsquedas de paquetes que tienen cierta característica. Para esto se debe seleccionar la opción Find Packet dentro del menú.

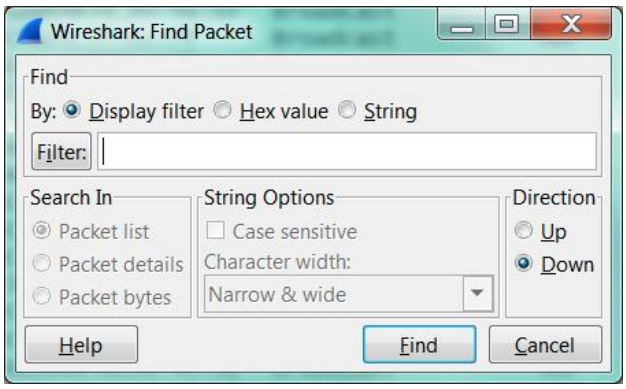


Ilustración 16 Buscador Paquetes – WireShark

Fuente: Software WireShark

3.2.3. Filtrado de Paquetes

Wireshark hace uso de libcap para la definición de filtros. Su sintaxis consta de una serie de expresiones conectadas por conjugaciones (and/or) con la opción de ser negada por el operador not.

Cuando es bien conocido el campo por el cual se requiere hacer el filtrado es recomendable hacer uso de Filter Expresion, facilitando la construcción de la expresión o fórmula seleccionado el campo, el operador y el valor contra el cual se requiere comparar.

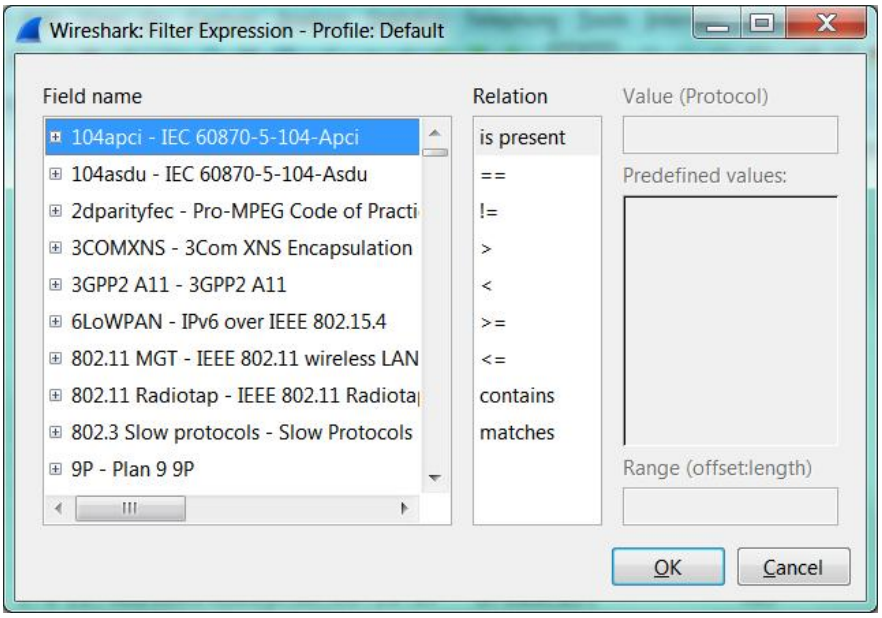


Ilustración 17 Filter Expresion – WireShark

Fuente: Software WireShark

Es muy común que ciertos filtros y/o expresiones requieran ser utilizados en un futuro, para esto WireShark permite definir los filtros y/o expresiones y guardarlas.

3.2.4. Manipulación y Análisis de Paquetes Capturados

Una vez capturados los paquetes estos son listados en el panel de paquetes capturados, al seleccionar se despliegan en los paneles de detalle de paquetes y panel de bytes.

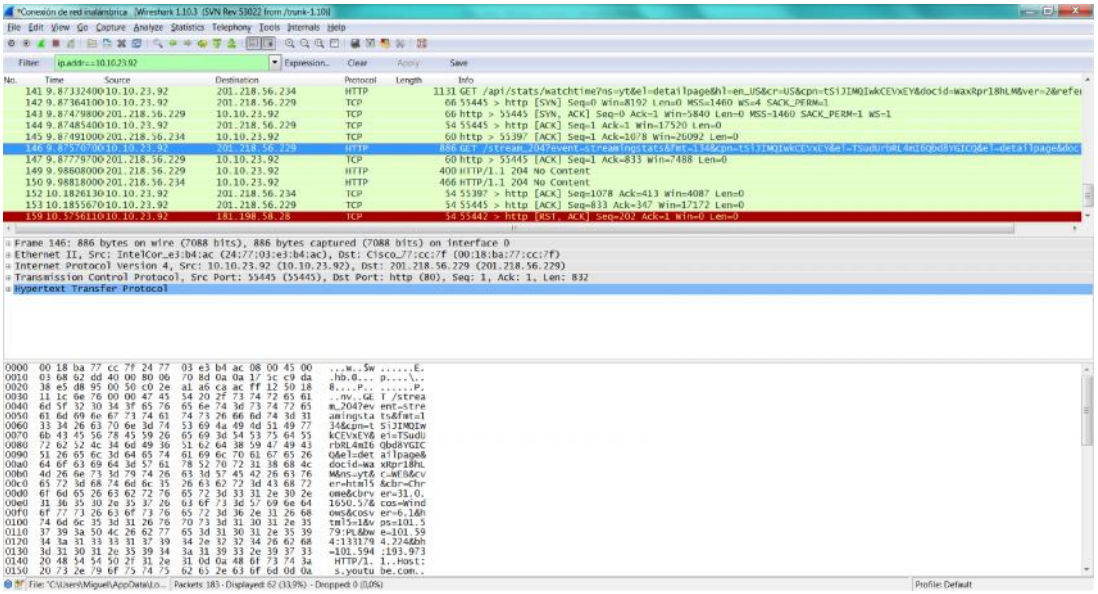


Ilustración 18 Captura de Paquetes – WireShark

Fuente: Software WireShark

Otra opción útil dentro de este aplicativo es poder filtrar por el tipo de protocolo que se desee monitorear, por ejemplo http, arp, ip.

La segunda zona muestra los datos del Frame capturado. En el caso de la imagen el Frame o captura 146 que se muestra en la Ilustración 19 que son enumerados secuencialmente. Nos da la información de todos los protocolos involucrados en la captura.

Ilustración 19 Frame Capturados – WireShark

Fuente: Software WireShark

En campo Frame como se muestra en la Ilustración 19 nos muestra información completa de la trama capturada, fecha y hora de la captura, número, longitud de las capturadas, protocolos encontrados. Luego Ethernet II muestra la cabecera que a su vez pertenece a la capa de enlace de datos.

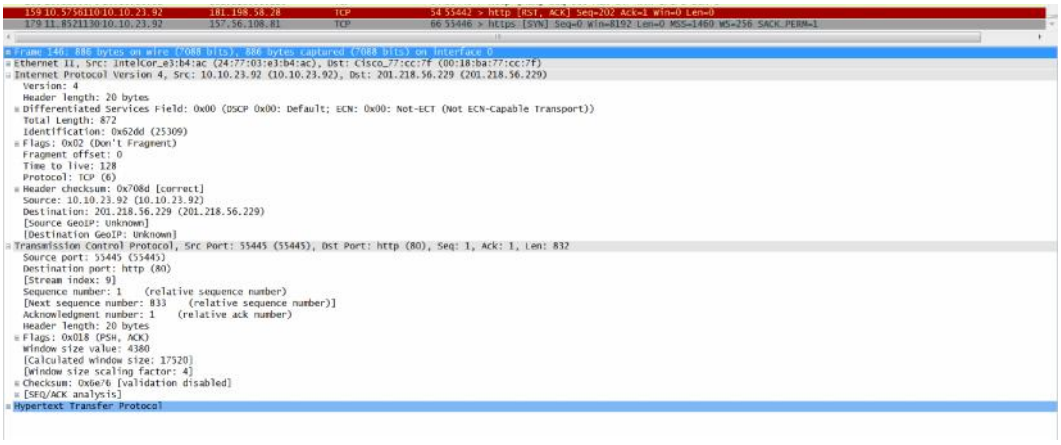


Ilustración 20 Datagrama - TCP – WireShark

Fuente: Software WireShark

A continuación se ve Internet Protocol con los datos de la cabecera del datagrama IP.

Después se encuentra la Transmission Control Protocol (TCP) de acuerdo a la Ilustración 20, el cual se trata del segmento TCP, protocolo involucrado en la captura de ejemplo, la cual tiene la información del puerto origen, destino, número de secuencia, checksum, etc.

Finalmente está TCP Segment Data Ilustración 21, con todo el contenido del campo Data del segmento TCP.

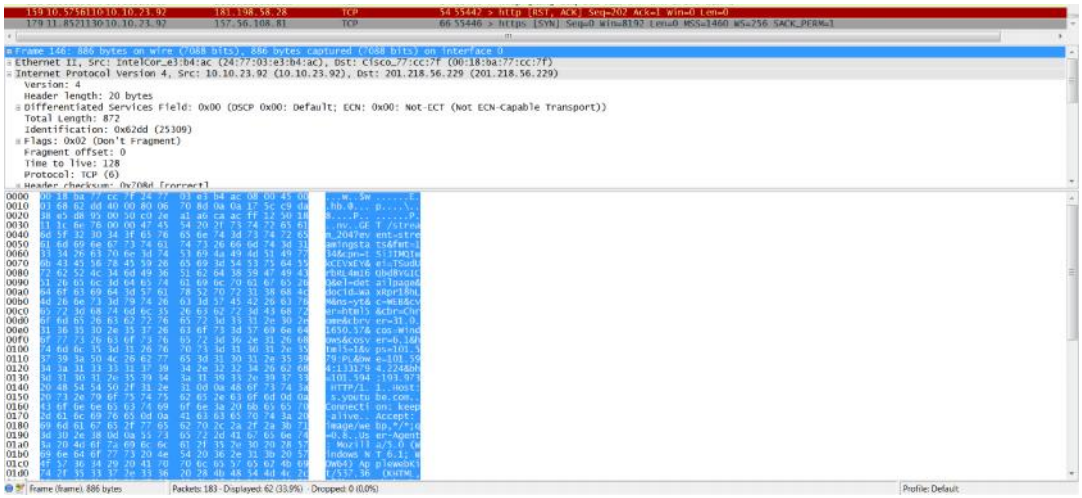


Ilustración 21 Contenido Paquete – WireShark

Fuente: Software WireShark

3.2.5. Interpretación de los Datos

En las capturas de pantallas se ve la posición del paquete, el timestamp del paquete, dirección origen del paquete, dirección destino del paquete, nombre del protocolo del paquete, información adicional del contenido del paquete.

En la captura de tráfico se presenta en la columna de protocolos TCP, ARP, MSNMS (MSN Messenger Service), SMB (Server Message Block), SSDP

(Simple Service Discovery Protocol), LLMNR (Link Local Multicast Name Resolution).

Se puede rastrear el uso del Messenger, de internet, de transferencias de archivos, se ve mensajes de errores cuando un servicio no está disponible o cuando un host no puede ser encontrado, además de la compartición de archivos.

CAPITULO IV

4.1. Evaluación del Cumplimiento de la Norma en la Universidad Tecnológica Equinoccial

4.1.1. Antecedentes

El propósito de este capítulo es desarrollar la evaluación de la seguridad de la información de los datos de tarjeta de crédito a través de un análisis forense.

Llamando análisis forense a los pasos a realizar para obtener la evidencia la cual será la información de tarjetas de crédito a través de la captura de datos y análisis de los mismos mediante herramientas propias para análisis forense en base a la norma PCI-DSS como una tarea preventiva, mediante la evaluación de los diferentes requisitos expuestos en la misma.

Se determinará un nivel de cumplimiento de la institución a nivel general de todos los controles de PCI-DSS. Teniendo presente que el estándar está compuesto por controles tanto físicos, lógicos, así también administrativos y documentales, con lo cual se realizará un trabajo profundo basado en ciertos puntos en la matriz de cumplimiento de la norma PCI-DSS los cuales son:

Tabla 3 Requisitos - Pesos del Requerimiento

Requisitos PCI DSS	Peso del Requerimiento
Requerimiento 3: Proteger los datos del titular de la tarjeta	
3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos, como se indica: 3.1.1 Implemente una política de retención y disposición de datos que incluya: § Limitación del almacenamiento de datos y del tiempo de retención a la cantidad exigida por los requisitos legales, reglamentarios y del negocio § Procesos para eliminar datos de manera cuando ya no se necesiten § Requisitos de retención específicos para datos de titulares de tarjetas § Un proceso automático o manual trimestral para identificar y eliminar de manera segura los datos de titulares de tarjetas almacenados que excedan los requisitos de retención definidos	1
3.2 No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). Los datos confidenciales de autenticación incluyen los datos mencionados en los requisitos 3.2.1 a 3.2.3, establecidos a continuación: Nota: Es posible que los emisores de tarjetas y las empresas que respaldan los servicios de emisión almacenen datos confidenciales de autenticación si existe una justificación de negocio y los datos se almacenan de forma segura.	1
3.2.1 No almacene contenido completo de ninguna pista de la banda magnética (ubicada en el reverso de la tarjeta, datos equivalentes que están en un chip o en cualquier otro dispositivo). Estos datos se denominan alternativamente pista completa, pista, pista 1, pista 2 y datos de banda magnética. Nota: En el transcurso normal de los negocios, es posible que se deban retener los siguientes elementos de datos de la banda magnética: § El nombre del titular de la tarjeta § Número de cuenta principal (PAN) § Fecha de vencimiento § Código de servicio Para minimizar el riesgo, almacene solamente los elementos de datos que sean necesarios para el negocio.	1
3.2.2 No almacene el valor ni el código de validación de tarjetas (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de pago) que se utiliza para verificar las transacciones de tarjetas ausentes.	1
3.2.3 No almacene el número de identificación personal (PIN) ni el bloqueo del PIN cifrado.	1

CONTINUA

3.3 Oculte el PAN cuando aparezca (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá).	5
3.4 Haga que el PAN quede ilegible en cualquier lugar donde se almacene (incluidos los datos que se almacenen en medios digitales portátiles, en medios de copia de seguridad y en registros) utilizando cualquiera de los siguientes métodos: § Valores hash de una vía basados en criptografía sólida (el hash debe ser de todo el PAN). § Truncamiento (los valores hash no se pueden usar para reemplazar el segmento truncado del PAN) § Tokens y ensambladores de índices (los ensambladores se deben almacenar de manera segura). § Sólida criptografía con procesos y procedimientos de gestión de claves relacionadas. Nota: Para una persona maliciosa sería relativamente fácil reconstruir el PAN original si tiene acceso tanto a la versión truncada como a la versión en valores hash de un PAN. Si el entorno de una entidad tiene versiones en valores hash y truncada del mismo PAN, se deben implementar controles adicionales para asegurar que las versiones en valores hash y truncada no se puedan correlacionar	5
Requerimiento 4: Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.	
4.2 Nunca debe enviar PAN no cifrados por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea, el chat, etc.).	2
Requerimiento 6: Desarrolle y mantenga sistemas y aplicaciones seguras	
6.3 Desarrolle aplicaciones de software (acceso interno y externo, e incluso acceso administrativo basado en la web a aplicaciones) de conformidad con las PCI DSS (por ejemplo, autenticación segura y registro), basadas en las mejores prácticas de la industria. Incorpore seguridad de la información en todo el ciclo de vida de desarrollo del software. Estos procesos deben incluir lo siguiente:	3
6.3.2 Revisión del código personalizado antes del envío a producción o a los clientes a fin de identificar posibles vulnerabilidades de la codificación. Nota: Este requisito de revisión de códigos se aplica a todos los códigos personalizados (tanto internos como públicos) como parte del ciclo de vida de desarrollo del sistema. Las revisiones de los códigos pueden ser realizadas por terceros o por personal interno con conocimiento. Las aplicaciones web también están sujetas a controles adicionales, si son públicas, a los efectos de tratar con las amenazas continuas y vulnerabilidades después de la implementación, conforme al Requisito 6.6 de las PCI DSS.	3
6.4 Siga los procesos y procedimientos de control de todos los cambios en los componentes del sistema. Los procesos deben incluir lo siguiente: 6.4.1 Desarrollo/prueba por separado y entornos de producción	3

CONTINUA

6.4.2 Separación de funciones entre desarrollo/prueba y entornos de producción	3
6.4.3 Los datos de producción (PAN activos) no se utilizan para las pruebas ni para el desarrollo	3
6.4.4 Eliminación de datos y cuentas de prueba antes de que se activen los sistemas de producción	3
6.4.5 Procedimientos de control de cambios para la implementación de parches de seguridad y modificaciones del software. Los procedimientos deben incluir lo siguiente: 6.4.5.1 Documentación de incidencia.	6
6.4.5.2 Aprobación de cambio documentada por las partes autorizadas.	6
6.4.5.3 Verifique que la prueba de funcionalidad se haya realizado para verificar que el cambio no incide de forma adversa en la seguridad del sistema.	6
6.4.5.4 Procedimientos de desinstalación.	6
6.5 Desarrolle aplicaciones basadas en directrices de codificación seguras. Evite vulnerabilidades de codificación comunes en los procesos de desarrollo de software, a fin de incluir: Nota: Las vulnerabilidades que se enumeran desde el punto 6.5.1 hasta el 6.5.9 eran congruentes con las mejores prácticas de la industria cuando se publicó esta versión de las PCI DSS. Sin embargo, debido a que las mejores prácticas de la industria para la gestión de vulnerabilidades se actualizan (por ejemplo, OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), se deben utilizar las mejores prácticas actuales para estos requisitos.	3
6.5.1 Errores de inyección, en especial, errores de inyección SQL. También considere los errores de inyección de comandos de OS, LDAP y Xpath, así como otros errores de inyección.	3
6.5.2 Desbordamiento de buffer	3
6.5.3 Almacenamiento cifrado inseguro	3
6.5.4 Comunicaciones inseguras	3
6.5.5 Manejo inadecuado de errores	3
6.5.6 Todas las vulnerabilidades —altas‖ detectadas en el proceso de identificación de vulnerabilidades (según lo definido en el Requisito 6.2 de las PCI DSS). Nota: Este requisito se considera una mejor práctica hasta el 30 de junio de 2012, y a partir de entonces se convierte en requisito.	3
Nota: Los requisitos del 6.5.7 al 6.5.9, que siguen, se aplican a las aplicaciones basadas en la web y a las interfaces de aplicaciones (internas o externas):: 6.5.7 Lenguaje de comandos entre distintos sitios (XSS)	3
6.5.8 Control de acceso inapropiado (tal como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios)	3
6.5.9 Falsificación de solicitudes entre distintos sitios (CSRF)	3
Requerimiento 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora	
8.1 Asigne a todos los usuarios una ID única antes de permitirles tener acceso a componentes del sistema o a datos de titulares de tarjetas.	4

CONTINUA

8.2 Además de la asignación de una ID única, emplee al menos uno de los métodos siguientes para autenticar a todos los usuarios: § Algo que el usuario sepa, como una contraseña o frase de seguridad § Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente § Algo que el usuario sea, como un rasgo biométrico	4
Requerimiento 9: Restringir el acceso físico a los datos del titular de la tarjeta	
9.1.2 Restrinja el acceso físico a conexiones de red de acceso público. Por ejemplo, las áreas que sean accesibles a los visitantes no deben tener puertos de red habilitados a menos que se autorice explícitamente el acceso a la red.	2
9.1.3 Limite el acceso físico a los puntos de acceso inalámbricos, gateways, dispositivos manuales, hardware de redes/comunicaciones y líneas de telecomunicaciones.	2
9.7.2 Envíe los medios por correo seguro u otro método de envío que se pueda rastrear con precisión.	5
Requerimiento 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas	
10.3 Registre al menos las siguientes entradas de pistas de auditoría de los componentes del sistema para cada evento: 10.3.1 Identificación de usuarios	4
10.3.2 Tipo de evento	4
10.3.3 Fecha y hora	4
10.3.4 Indicación de éxito o fallo	4
10.3.5 Origen del evento	4
10.3.6 Identidad o nombre de los datos, componentes del sistema o recurso afectados.	4
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. 10.4.1 Los sistemas críticos tienen horario uniforme y correcto.	4
10.4.2 Los datos de tiempo están protegidos.	4
10.4.3 La configuración de tiempo se recibe de fuentes aceptadas por la industria.	4
10.5 Resguarde las pistas de auditoría para evitar que se modifiquen. 10.5.1 Limite la visualización de pistas de auditoría a quienes lo necesiten por motivos de trabajo.	4
10.5.2 Proteja los archivos de las pistas de auditoría contra las modificaciones no autorizadas.	4
10.5.3 Realice copias de seguridad de los archivos de las pistas de auditoría de inmediato en un servidor de registros central o medios que resulten difíciles de modificar.	4
10.5.4 Escriba registros para tecnologías que interactúen con la parte externa en un servidor de registros en la LAN interna.	4
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).	4

CONTINUA

10.6 Revise los registros de todos los componentes del sistema al menos una vez al día. Las revisiones de registros incluyen a los servidores que realizan funciones de seguridad, tales como sistema de detección de intrusiones (IDS) y servidores de autenticación, autorización y contabilidad (AAA) (por ejemplo, RADIUS).	4
10.7 Conserve el historial de pista de auditorías durante al menos un año, con un mínimo de tres meses inmediatamente disponible para el análisis (por ejemplo, en línea, archivado o recuperable para la realización de copias de seguridad).	4
Requerimiento 11: Pruebe con regularidad los sistemas y procesos de seguridad	
11.2Realice análisis internos y externos de vulnerabilidades de red al menos trimestralmente y después de cada cambio significativo en la red (tales como instalaciones de componentes del sistema, cambios en la topología de red, modificaciones en las normas de firewall, actualizaciones de productos). 11.2.1 Realice análisis de vulnerabilidad interna trimestralmente.	2
11.2.3 Realice análisis internos y externos después de cualquier cambio significativo.	2
11.3 Realice pruebas de penetración externas e internas al menos una vez al año y después de cualquier actualización o modificación significativa de infraestructuras o aplicaciones (como por ejemplo la actualización del sistema operativo, la adición de una subred al entorno, o la adición de un servidor Web al entorno). Estas pruebas de penetración deben incluir lo siguiente: 11.3.1 Pruebas de penetración de la capa de red	2
11.3.2 Pruebas de penetración de la capa de aplicación	2
11.4 Utilice los sistemas de detección y/o prevención de intrusiones para supervisar el tráfico en el perímetro del entorno de datos de titulares de tarjetas, así como los puntos críticos dentro del entorno de datos de titulares de tarjetas y alerte al personal ante la sospecha de riesgos.	2
11.5 Deploy file integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files or content files; and configure the software to perform critical file comparisons at least weekly.	4
Requerimiento 12: Mantenga una política que aborde la seguridad de la información para todo el personal	
12.1 Establezca, publique, mantenga y distribuya una política de seguridad que logre lo siguiente:	6
12.1.1 Aborda todos los requisitos de las PCI DSS.	1
12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	2
12.1.3 Incluye una revisión al menos una vez al año y actualizaciones al modificarse el entorno.	3
12.2 Desarrolle procedimientos diarios de seguridad operativa coherentes con los requisitos de esta especificación (por ejemplo, procedimientos de mantenimiento de cuentas de usuarios y procedimientos de revisión de registros).	4

CONTINUA

12.3 Desarrolle políticas de utilización para tecnologías críticas para empleados (por ejemplo, tecnologías de acceso remoto, tecnologías inalámbricas, dispositivos electrónicos extraíbles, computadoras portátiles, asistentes digitales/para datos personales [PDA], utilización del correo electrónico y de Internet) para definir el uso adecuado de dichas tecnologías. Asegúrese de que estas políticas de uso requieran lo siguiente: 12.3.1 Aprobación explícita por las partes autorizadas	5
12.3.2 Autenticación para el uso de la tecnología	6
12.3.3 Lista de todos los dispositivos y personal que tenga acceso	1
12.3.4 Etiquetado de dispositivos con propietario, información de contacto y objetivo	6
12.3.5 Usos aceptables de la tecnología	6
12.3.6 Ubicaciones aceptables de las tecnologías en la red	6
12.3.7 Lista de productos aprobados por la empresa	6
12.3.8 Desconexión automática de sesiones para tecnologías de acceso remoto después de un período específico de inactividad	6
12.3.9 La activación de las tecnologías de acceso remoto para proveedores y socios de negocios solo cuando es necesaria para proveedores y socios de negocios, con desactivación inmediata después del uso	6
12.3.10 Para que el personal tenga acceso a datos de titulares de tarjetas mediante tecnologías de acceso remoto, prohíba copiar, mover y almacenar los datos de titulares de tarjetas en unidades de disco locales y dispositivos electrónicos extraíbles, a menos que sea autorizado explícitamente para una necesidad de negocios definida..	6
12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todo el personal.	6
12.5 Asigne las siguientes responsabilidades de gestión de seguridad de la información a una persona o equipo:	6
12.5.1 Establezca, documente y distribuya políticas y procedimientos de seguridad.	6
12.5.2 Supervise y analice las alertas e información de seguridad, y distribúyalas entre el personal correspondiente.	6
12.5.3 Establezca, documente y distribuya los procedimientos de respuesta ante incidentes de seguridad y escalación para garantizar un manejo oportuno y efectivo de todas las situaciones.	6
12.5.4 Administre las cuentas de usuario, incluidas las adiciones, eliminaciones y modificaciones	6
12.5.5 Supervise y controle todo acceso a datos	6
12.6 Implemente un programa formal de concienciación sobre seguridad para que todos los empleados tomen conciencia de la importancia de la seguridad de los datos de titulares de tarjetas	6
12.6.1Eduque al personal justo al ser contratado y, por lo menos, una vez al año.	6
12.6.2 Exija a los empleados que reconozcan al menos una vez al año haber leído y entendido la política y los procedimientos de seguridad de la empresa.	4

CONTINUA

12.7 Examine a los empleados antes de contratarlos a fin de minimizar el riesgo de ataques desde fuentes internas. (Entre los ejemplos de verificaciones de antecedentes se incluyen el historial de empleo, registro de antecedentes penales, historial crediticio y verificación de referencias).	6
12.8 Si los datos de titulares de tarjeta se comparten con proveedores de servicios, mantenga e implemente políticas y procedimientos a los fines de que los proveedores de servicio incluyan lo siguiente:	6
12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	6
12.8.3 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso.	6
12.8.4 Mantenga un programa para supervisar el estado de cumplimiento con las PCI DSS del proveedor de servicios.	6
12.9 Implemente un plan de respuesta a incidentes. Prepárese para responder de inmediato ante un fallo en el sistema.	6
12.9.1 Cree el plan de respuesta a incidentes que será implementado en caso de que ocurra una violación de la seguridad del sistema. Asegúrese de que el plan aborde, como mínimo, lo siguiente: -Roles, responsabilidades y estrategias de comunicación y contacto en caso de un riesgo que incluya, como mínimo, la notificación de las marcas de pago. -Procedimientos específicos de respuesta a incidentes. - Procedimientos de recuperación y continuidad comercial. - procesos de realización de copia de seguridad de datos; - Análisis de los requisitos legales para el informe de riesgos. - Cobertura y respuestas de todos los componentes críticos del sistema. - referencia o inclusión de procedimientos de respuesta a incidentes de las marcas de pago.	2
12.9.2 Pruebe el plan al menos una vez al año.	2
12.9.3 Designe personal especializado que se encuentre disponible permanentemente (24/7) para responder a las alertas	2
12.9.4 Proporcione capacitación adecuada al personal sobre las responsabilidades de respuesta ante fallos de seguridad.	2
12.9.5 Incluya alertas de sistemas de detección y prevención de intrusiones, y de supervisión de integridad de archivos.	4
12.9.6 Elabore un proceso para modificar y desarrollar el plan de respuesta a incidentes según las lecciones aprendidas, e incorporar los desarrollos de la industria.	4
12.9.2 Test the plan at least annually.	4
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	4
12.9.4 Provide appropriate training to staff with security breach response responsibilities.	4
12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.	4
12.9.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	4

Además se realizará una búsqueda de potenciales datos de tarjeta almacenados en texto claro. Esta es la labor más importante, ya que el núcleo del estándar es la protección de datos de tarjetas procesados, visualizados (Req. 3.3), almacenados (Req, 3.4) y transmitidos (Req. 4). Para ello, se utilizará la herramienta Open Source WireShark que describe en este proyecto de tesis, ubicándose en términos lógicos entre puntos en comunicación, capturando una muestra y analizando los resultados buscando con patrones regulares.

4.2. Caso Práctico

4.2.1. Información Preliminar

En el presente capitulo se desarrollará el caso práctico, donde se aplicará el método de investigación de un análisis forense como también técnicas e instrumentos de recolección y procesamiento de datos e información.

Es así que la metodología a aplicar dentro del desarrollo de este proyecto es experimental y se basa prácticamente en cuatro elementos claves mostrados en la Ilustración 22 dentro del análisis forense los cuales son:

- Identificación
- Conservación
- Análisis
- Presentación

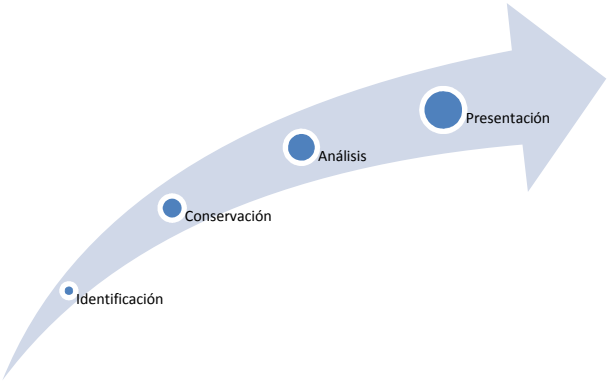


Ilustración 22 Metodología Análisis Forense

4.2.2. Introducción

La Universidad Tecnológica Equinoccial es una institución educativa particular sin fines de lucro, integrada por una comunidad universitaria competente, comprometida con la educación mediante propuestas innovadoras y con calidad.

La universidad cuenta con una estructura administrativa muy organizada en sus diferentes departamentos, áreas y servicios para el servicio de la comunidad. Entre los departamentos administrativos que cuenta la universidad y que es parte de la investigación del análisis forense son Tesorería, Contabilidad y Sistemas donde se desarrolla la gestión financiera institucional en forma integrada, con eficiencia, oportunidad y transparencia en el uso y manejo de los recursos financieros asignados a la Institución; así como dotar de información dentro de ésta área, al nivel superior en el proceso de toma de decisiones.

El departamento de tesorería como gestión financiera da el servicio a los estudiantes en el pago de aranceles de estudios como son: pregrado, posgrados y otros, en donde los pagos pueden ser mediantes cheques certificados, transferencia electrónica, órdenes de pago en moneda extranjera o moneda local y tarjetas de crédito.

Se ha visto la necesidad de verificar el servicio a nivel de seguridad a los estudiantes o personas que realizan sus pagos a través de tarjetas de crédito para establecer controles a nivel de tarjetas de crédito que eviten siniestros de perdida de información dentro de la institución y aseguren una mayor confidencialidad de la información, para esto se desea aplicar la normas PCI – DSS que fomenta y mejora la seguridad de los datos del tarjeta habiente y facilita la adopción de medidas de seguridad consistentes a nivel mundial.

El presente proyecto delimita su alcance exclusivamente en los requisitos 10 y 11 de la norma PCI – DSS que controla todos los accesos a los recursos de la red y los datos de los titulares de la tarjeta de crédito como también los procesos de seguridad.

4.2.3. Identificación

En la presente metodología determinarán las fuentes de información que se utilizaron como base para la extracción de la información.

La fuente de información es el lugar donde se encuentran los datos requeridos, que posteriormente se pueden convertir en información útil para la investigación. Estos datos, que se deben recopilar de las fuentes, tendrán que ser suficientes para poder sustentar y defender un trabajo (Eyssautier, 2002).

Es así que para la identificación se realizaron varios procesos descritos en la Ilustración 23.

Ilustración 23 Identificación de los Procesos

4.2.4. Entrevistas

La fuente primaria que se utilizó para todos los objetivos aquí planteados es el de entrevista, que se realizó a las diferentes áreas que se encuentran involucradas dentro del proceso de transacciones con tarjeta de crédito.

Es así que en esta fase se realiza la evaluación de las áreas y los recursos que son necesarios para realizar la investigación interna y además de cómo se están transmitiendo los datos por la red por las diferentes áreas además se realizó una pre-evaluación de cumplimiento de acuerdo a Declaración de cumplimiento de evaluaciones in situ de la normativa **Anexo 2**.

Como primer paso se identificó las áreas en donde los datos de la tarjeta de crédito son ingresados desde su inicio hasta cuando los datos son almacenados, tal como se indica en el **Anexo 3**.

4.2.4.1. Identificación del Proceso de Transacciones de Pago con Tarjetas de Crédito

De acuerdo a las conversaciones que se mantuvo con los funcionario del Departamento de Tesorería y Contabilidad, con el propósito de conocer el proceso, se inicia el procedimiento desde cuando el estudiante va a cancelar su arancel estudiantil mediante la tarjeta de crédito describiendo como ingresa la

información a través del sistema de la Universidad hasta cuando la información se almacena en el departamento de sistemas.

Luego se realizó la entrevista al Administrador de la red (**Anexo 4**), para poder identificar, evaluar y verificar la segmentación de la red.

4.2.4.2. Análisis de Red y Aplicativo

Segmentación de la red de las áreas afectadas de la Universidad Tecnológica Equinoccial

Como punto preliminar se identificó que la segmentación de la red (Ilustración 24), del entorno de los datos del titular de la tarjeta del resto de la red de la Universidad Tecnológica Equinoccial no constituye un requisito de las PCI-DSS. Sin embargo, lo utilizaremos dentro de este proyecto como un método en el cual vamos poder disminuir:

- El alcance de la evaluación de las PCI DSS
- El costo de la evaluación de las PCI DSS
- El costo y la dificultad de la implementación y del mantenimiento de los controles de las PCI DSS
- El riesgo de la Universidad ya que, gracias a la consolidación de los datos del titular de la tarjeta en menos y más controladas ubicaciones, se ve reducido.

Sin la adecuada segmentación de la red, toda la red se encuentra dentro del alcance de la evaluación de las PCI DSS, la segmentación de la red se puede alcanzar mediante diversos medios físicos o lógicos, tales como firewalls internos de red, routers con sólidas listas de control de acceso u otras tecnologías con la apropiada configuración que restrinjan el acceso a un segmento particular de la red.

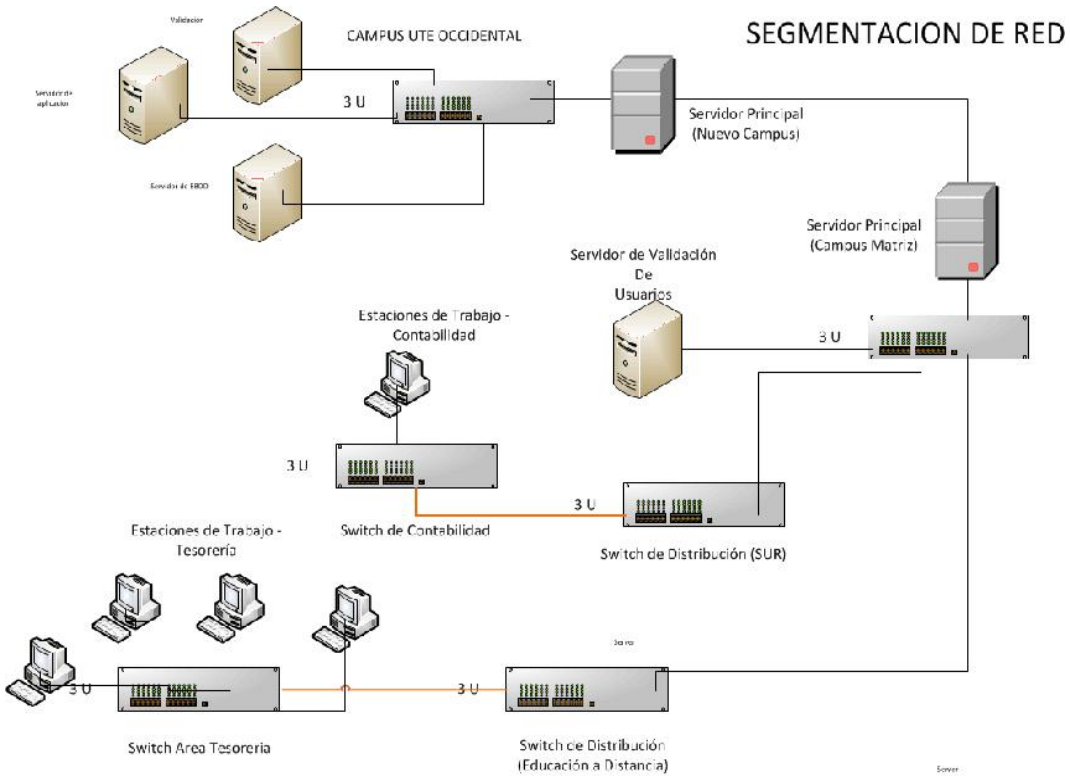


Ilustración 24 Segmentación de la Red

A continuación se detalla cómo está constituida la red en las áreas de tesorería, contabilidad y sistemas.

En un área o departamento siempre existe una red informática que está compuesta por computadoras que están conectados entre sí mediante líneas de comunicación (cables de red) y equipos de hardware (adaptadores de red), a esto le llamamos como configuración de red de datos o topología física.

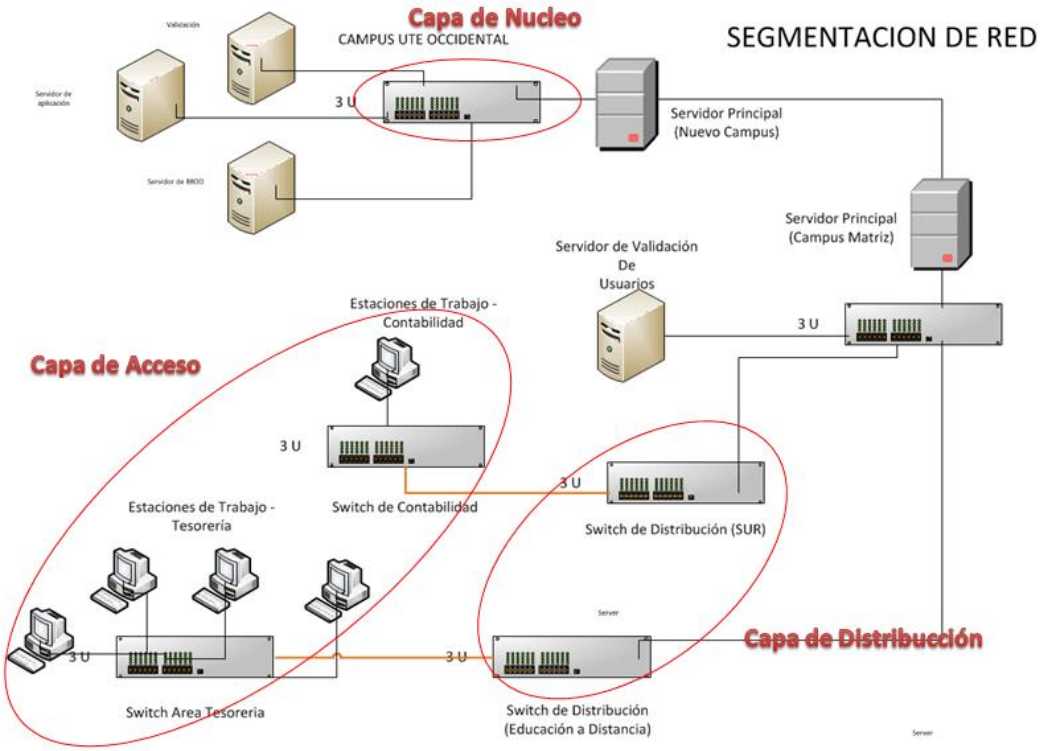
Dentro de la Universidad Tecnológica Equinoccial y en las áreas de análisis de tesorería y contabilidad se maneja la topología física estrella en donde las máquinas están conectadas a un concentrador llamado switch que tiene la tarea de enviar mensajes a cada uno de los puertos para la comunicación a cada equipo.

Dentro de esta red de cómputo existen varios tipos de elementos que la integran, estos elementos ya sea finales o intermedios, sirven de fuente de información útil para la realización del análisis forense. Como se está haciendo el estudio de la red interna en las áreas de tesorería y contabilidad implica que debe contener componentes de transmisión y de seguridad como routers, firewalls, ID´S y switchs, pero en este caso dentro de la Universidad, no existe los componentes de routers, firewalls ni ID´S ya que internamente dentro de la Universidad no existe un control de seguridad a nivel de transmisión de datos.

El único componente como transmisión de datos está el switch el cual maneja una segmentación de subred y redes virtuales (VLAN´S) esto permite un mejor control y manejo en la red.

Dentro de la Universidad se maneja el modelo jerárquico de red como se indica en la Ilustración 25, la cual consta de 3 capas:

- Capa de Acceso,
- Capa de Distribución, y
- Capa Núcleo



Capa de Acceso

En la capa de acceso está compuesta por las capas Física y de Enlace de acuerdo al Modelo TCP/IP, la capa física en donde se determina las características físicas de la comunicación, como también se sobreentiende por naturaleza los medios físicos que intervienen en la comunicación (comunicación por cable Ethernet, fibra óptica, etc.) y los demás como relativo los detalles de conectores, canaletas entre otros. En la capa de enlace en donde se detalla cómo son transmitidos los paquetes sobre el nivel físico, incluyendo los delimitadores. Dentro de la Universidad esta capa se refiere a la comunicación de las maquinas hacia los switch de acceso que serían los switch de contabilidad y tesorería mediante tramas, las mismas que incluyen cabeceras o identificadores de la maquina o máquinas de la red.

Capa de Distribución

En la capa de distribución comprende únicamente la capa de enlace de acuerdo al modelo TCP/IP, en donde la comunicación se la realiza por medio de las MAC entre los switch de la capa de acceso hacia los switch de Distribución (Sur y de Educación a Distancia).

Capa de Núcleo

Esta capa comprende la capa de Red de acuerdo al modelo TCP/IP, aquí se maneja la transmisión de datos mediante direccionamiento lógico que viene a ser las ip's de los equipos, dentro de la Universidad se manejan los switch de capa tres donde los paquetes transmitidos desde la capa de distribución hacia los switch de core tanto de la matriz como del campus occidental para ser almacenados dentro de los servidores.

Cabe resaltar que cada capa hace el proceso de encapsulamiento y des encapsulamiento de datos.

Además queda implícitamente relacionado en las tres capas descritas anteriormente la capa de Transporte que es la 4 capa de acuerdo al modelo TCP/IP en donde permite solucionar los problemas de fiabilidad del destino correcto de los paquetes de datos como lo es los datos de la tarjeta de crédito como también la seguridad de estos datos.

Así también cabe indicar que la transmisión de datos dentro de la Universidad entre las diferentes capas de la red se lo realiza a 100 Megabits por segundo, y la velocidad de comunicación entre las capas de distribución y núcleo es de 1 Gigabit.

El ancho de banda esta categorizada por 5e, 6 y 6a, dentro del campus Matriz se maneja el 65% de categoría 5e y el 35 % se encuentra dentro de las categorías 6 y 6ª.

Y como quinta capa de acuerdo al modelo TCP/IP está la de aplicación en donde directamente esta la aplicación o el sistema integrado (SICAF) que se comunica mediante la red hacia el destino que en este caso seria los servidores de almacenamiento siendo como el inicio del proceso del pago con tarjeta de crédito.

Este análisis de las capas TCP/IP están en función al proceso que se maneja las áreas de tesorería y contabilidad y sistemas, y además al análisis que se realizó para estructurar la segmentación interna de la red que comprende la universidad.

Dentro del estudio de la segmentación de la red dentro del área de tesorería se detalla que cuenta con 4 ventanillas de atención, el cual está asignada por una persona responsable con su computadora para la atención al usuario, cada computador está integrado a la red a través del sistema integrado SICAF siendo este como inicio del proceso de ingreso de datos de la tarjeta.

Aplicativo Sistema SICAF (Sistema Integrado Control Académico Financiero)

De acuerdo a las entrevistas realizadas se identificó que el proceso de cobro de los aranceles de la Universidad Tecnológica Equinoccial inicia desde el aplicativo SICAF (Sistema Integrado Control Académico Financiero) Ilustración 26, el mismo que entro dentro del proceso de evaluación para poder determinar los campos que se almacena a través del sistema, para lo cual se realizó una captura de pantalla en donde se reconoció que por el aplicativo se almacenan el número de tarjeta de crédito y el nombre del titular de la tarjeta.

Distinguiendo que al momento de almacenar los datos de una transacción dentro del aplicativo no se realiza ninguna acción de resguardo de información en lo referente a tarjeta de crédito, como por ejemplo el número de tarjeta de crédito se digita y no se realiza ningún tipo de cifrado de datos.

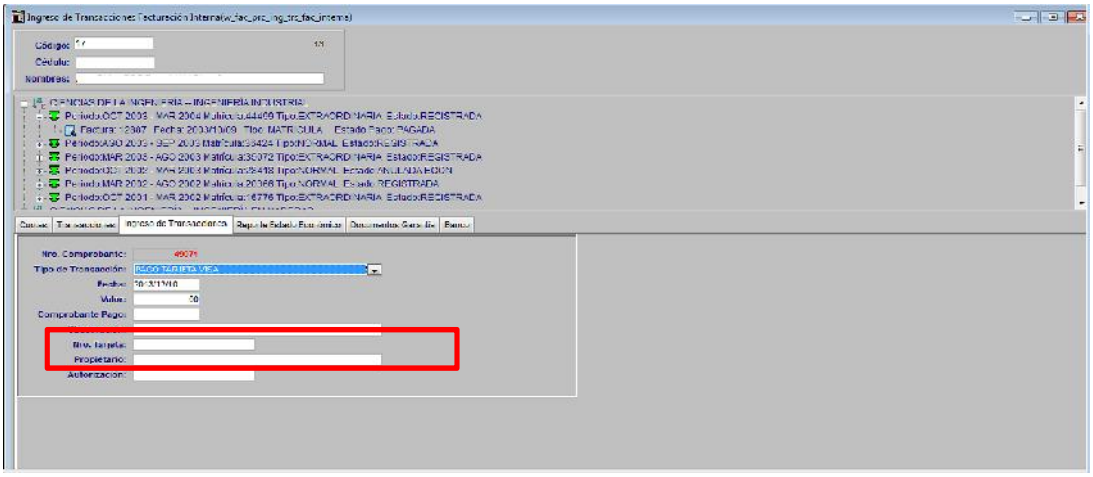


Ilustración 26 Aplicativo SICAF

4.2.4.3. Captura de Datos a través del Sniffer

La utilidad del sniffer nos abre las posibilidades para realizar el análisis forense dentro de la red de la universidad

En función del tiempo que empleamos en nuestras sesiones de sniffing, trataremos de recolectar información sobre tarjetas de crédito y tarjeta habientes que realizan transacciones dentro de la Universidad, las cuales posteriormente serán analizadas.

Para la identificación de los puntos se basó en el diseño de la red que tiene la Universidad en donde la red está compuesta por capas independientes, cada capa cumple roles específicos haciendo esto una red modular facilitando la escalabilidad y el rendimiento. Como se mencionó anteriormente las capas de una red jerárquica son tres: capa de acceso, capa de distribución y capa núcleo.

Dentro de la Universidad Tecnológica Equinoccial la arquitectura de la LAN está basada bajo los principios de una red jerárquica con sus respectivos modelos de switchs Cisco que están conectados en cada capa de red.

Con esta red jerárquica que mantiene la Universidad, se expande con más facilidad y los problemas se resuelven con mayor rapidez y además nos ayuda

para nuestra investigación en la identificación de los puntos importantes para el análisis de los datos.

Como parte de la identificación y análisis de los puntos para la captura de los datos, se identificó sitios que están dentro de las 3 capas que compone una red jerárquica y que son fundamentales para la transmisión de datos e ideales para la captura de paquetes o tramas que se generan desde el departamento de tesorería siendo este el punto de partida para la generación de la transacción de pago con tarjetas de crédito.

Es así que para realizar las capturas de datos en la red de la universidad, nos basamos en la segmentación de la red identificada previamente, con lo cual se reconoció 6 puntos para poder conectar el sniffer y capturar datos.

- Punto 1 Switch Campus UTE Occidental
- Punto 2 Switch Principal Campus Matriz
- Punto 3 Switch de Distribución (Sur)
- Punto 4 Switch Área Contabilidad
- Punto 5 Switch de Distribución Educación a Distancia
- Punto 6 Switch Área Tesorería

La captura de datos o paquetes se lo realizo mediante el software WireShark la cual captura tramas Ethernet, colocando un equipo para capturar los datos en cada punto descrito anteriormente que se indica en la Ilustración 27, teniendo en cuenta que el escenario de pruebas se basa en la transmisión de datos de tarjetas de crédito y la información de tarjeta habientes.

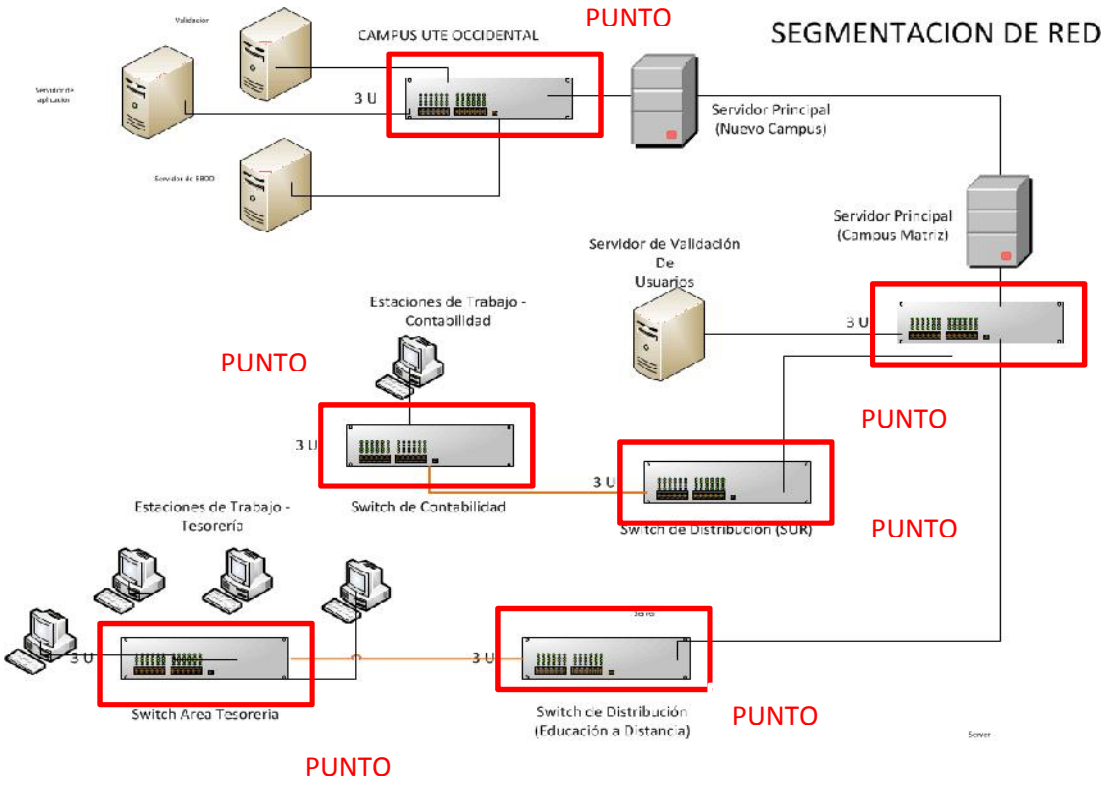


Ilustración 27 Aplicación de Sniffers - Red Segmentada

El equipo verificador se conectó en cada switch de las capas de acceso, de distribución y los de núcleo.

Se seleccionaron estos puntos para la obtención de datos por los siguientes motivos:

Punto 1 que es la capa de núcleo y que además cuenta con un switch Cisco 6500, es el punto principal ya que todos los datos y la información que se genera en los puntos que se describirán posteriormente del Campus Matriz de la Universidad llegan a este punto siendo estos almacenados en los servidores de la Universidad.

Este switch tiene la siguiente funcionalidad:

- Son de alto rendimiento y eficiencia operativa

- Implementa hasta 96 puertos 40 GE o 384 puertos 10 GE en un factor de forma pequeño de cuatro unidades de rack (RU)
- Ofrecen funcionalidad completa integrada de capa 2 y 3 a velocidad de cable y con baja latencia
- Mejoran la eficiencia mediante compatibilidad con la arquitectura con la arquitectura de extensor de estructura de Cisco (CIsco FEX) y un completo kit de herramientas analíticas
- Compatibles con canal de fibra por Ethernet (FCoE) de 40 GE para convergencia de redes LAN y SAN
- Son ideales para implementaciones de agregación de acceso y con limitaciones de espacio

Punto 2 que de igual manera es un switch de distribución Cisco 4500 cumpliendo con la misma función del punto anterior, pero con la particularidad de que a este switch le llegan los datos de los puntos 3 y 5 y este a la vez se comunica con el switch principal que está en el punto 1 que es el centro de cómputo que está en el Nuevo Campus.

Puntos 3 y 5 que están en la capa de distribución y que además cuentan con switchs de distribución Cisco 4500, estos se conectan a los switchs de acceso para manejar una mejor escalabilidad y además proporcionan una mejor comunicación entre las áreas de tesorería y el área de contabilidad.

Punto 4 que es el departamento de Contabilidad se identificó que al comienzo de la jornada de labores la persona que está encargada de sacar el reporte de los datos del sistema SICAF que se generó el día anterior en tesorería para ser verificada si los datos fueron ingresados correctamente y estos ser enviados al banco correspondiente.

De acuerdo al análisis realizado de las capas de acceso que comprende los puntos 4 y 6 como se indica en la Ilustración 27 en donde está el departamento de tesorería y contabilidad el cual cuenta con un switchs Cisco 2960 que son

apropiados para lo que es el acceso aportando como medio de conexión de los dispositivos a la red y además cuenta con las siguientes funcionalidades**:**

- Soporte para comunicaciones de datos, inalámbricas y voz que le permite instalar una única red para todas sus necesidades de comunicación
- Capacidad de Power over Ethernet para que puedan implementar nuevas funcionalidades como voz y tecnología inalámbrica sin tener que realizar un nuevo cableado
- Opción de Fast Ethernet (transferencia de datos de 100 Mbps) o Gigabit Ethernet (transferencia de datos de 1000 Mbps)
- Capacidad de configurar LANs virtuales de forma que los empleados estén conectados a través de funciones de organización, equipos de proyecto o aplicaciones en lugar de por criterios físicos o geográficos
- Seguridad integrada
- Funciones de monitorización de red y solución de problemas de conectividad mejoradas.

Finalmente el **Punto 6** que es el departamento de tesorería se genera el pago de uno o varios aranceles académicos bajo la transacción de tarjetas de crédito siendo el inicio del proceso de captura de datos hasta llegar hacia los servidores principales como punto final de la finalización del proceso en el que el alumno termina su proceso de pago.

Es así que para realizar la captura de paquetes la tarjeta de red del equipo verificador que capturará los datos se la configuró en modo promiscuo la cual habilita que la tarjeta de red acepte todo tipo de tráfico.

4.2.5. Conservación

Al ya tener los datos capturados mediante la herramienta WireShark la cual fue analizada y descrita sus características en el capítulo anterior se ejecutan las siguientes acciones: como primer paso para la preservación de la evidencia es

realizar dos copias de los datos obtenidos para realizar el análisis sobre una de ellas y a la otra mediante la herramienta TrueCrypt (Ilustración 28) cifrar una de las evidencias.

Se escogió a TrueCrypt ya que es una aplicación gratuita, dentro de sus características permite crear volúmenes cifrados (ya se trate de un disco virtual contenido en un fichero, una partición de disco o una unidad de almacenamiento USB), de tal forma que únicamente se puede acceder si se conoce la contraseña y/o fichero clave que se usó para la creación. Además de no ocupar mucho espacio en disco y fácil de instalar, Además usa diferentes algoritmos de cifrado, TrueCrypt está disponible tanto en Windows como en Linux.

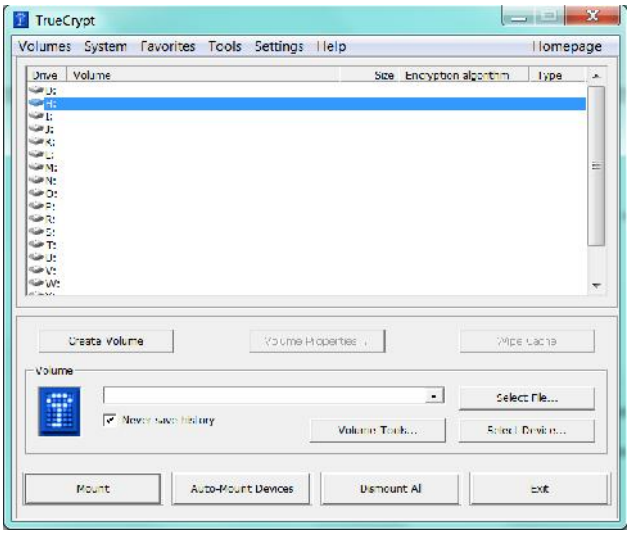


Ilustración 28 TrueCrypt

Fuente: Software TrueCrypt

Otro aspecto tomado en cuenta es el proceso conocido como cadena de custodia para establecer las responsabilidades y controles entre las personas que manipulamos los datos recogidos, los cuales como ejecutores de este proyecto de tesis nos responsabilizamos de los datos capturados y su correspondiente manipulación, además que los datos no sean expuestos a terceros para su mala utilización.

Con estas medidas logramos que el acceso a la evidencia sea muy restrictivo, posibilitando detectar y pedir responsabilidades ante manipulaciones incorrectas e intentos no autorizados.

4.2.5.1. Análisis Forense con Herramientas

Una vez que se dispone de los datos capturados y almacenados de forma adecuada, se continúa a la siguiente fase más laboriosa dentro del Análisis Forense propiamente dicho.

El análisis se dará por concluido cuando se encuentre dentro de la captura de datos, información de número de tarjetas de crédito.

4.2.5.2. Filtrado / Reducción de los datos para análisis con Wireshark

Dentro del análisis, es necesario realizar acciones sobre los datos a analizar, fue necesario ejecutar procedimientos para centrarse únicamente en datos potenciales. Este proceso de filtrar datos irrelevantes, confidenciales o privilegiados incluye:

- Identificar información válida y descartar la que no tiene relevancia en la investigación
- Enfocar el análisis en los datos que pueden contener la información necesario para la investigación como los número de bines de las tarjetas de crédito o débito.

Como primera tarea se realizó filtros de búsqueda en el aplicativo WireShark mediante las ip’s identificadas de las estaciones de trabajo como se mostró en la Ilustración 29, las cuales son las siguientes:

- Maquina 1: 172.17.2.148,
- Maquina 2: 172.17.2.155,
- Maquina 3: 172.17.2.81,
- Maquina 4: 172.17.1.93

Pero el resultado no fue favorable ya que no se pudo localizar ningún dato sobre tarjeta de crédito.

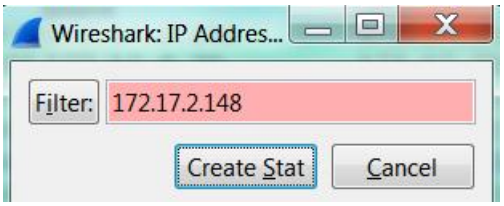


Ilustración 29 Filtro IP

La siguiente búsqueda se la realizo usando el listado que se encuentra en el Anexo 1 de los bines de tarjetas de crédito como expresiones regulares (Ilustración 30) para realizar búsquedas de patrones de tarjetas. Pero se enfrenta a múltiples problemas:

Alto número de registros falsos positivos: Ya que la búsqueda con expresiones regulares simplemente ubica cadenas que coincidan con un patrón dado, los resultados pueden tener un gran numero tasa de falsos positivos (números que tienen el mismo formato de un PAN pero que explícitamente no lo son).

Exclusiones: Al realizar la búsqueda con números fijos de los bines de tarjeta de crédito se encontró coincidencias dentro del archivo como por ejemplo los números de paquetes, los mismos que deben ser excluidos de la búsqueda.

Formatos y separadores: Cada marca tiene sus propias políticas respecto al formato de sus tarjetas (13, 14, 15, 16 dígitos de longitud). Igualmente, éstas pueden ser almacenadas empleando separadores como puntos, guiones, espacios, comas, etc. con lo cual si la expresión regular no es bien definida, estos datos se pueden pasar por alto y permanecer desprotegidos.

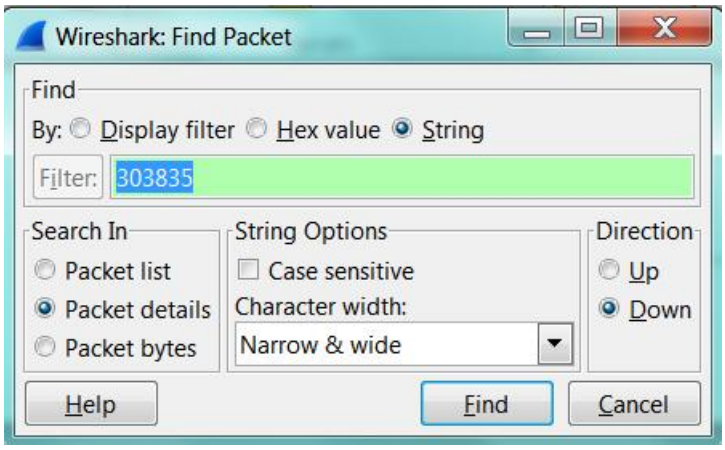


Ilustración 30 Búsqueda Patrones Regulares

Es así que con la herramienta WireShark no se pudo encontrar ningún número de tarjeta de crédito, únicamente se encontró falsos positivos.

Posteriormente se investigó herramientas de análisis forense que faciliten la búsqueda de números de tarjetas de crédito en archivos en formato *.pcap que se obtuvo con el software WireShark entra las que tenemos BreachProbe y CCSRCH.

BreachProbe

Es un software gratuito para la realización de análisis forense, el cual trabaja de la siguiente manera: extrae datos de la tarjeta de crédito y la información de sesión de red de archivos pcap y analiza los datos capturados. BreachProbe permitió importar archivos pcap capturados desde WireShark, por lo cual como primera acción se tuvo que transformar el archivo pcapng a PCAP ya que este formato contiene mayor información sobre la captura, como el momento, estadísticas, nombres resueltos, comentarios entre otros. El programa exporta los datos analizados en un archivo de registro y automáticamente genera un hash

SHA256 de los datos exportados. Sólo los últimos cuatro dígitos del número de tarjeta de crédito se almacenan en el archivo de registro. BreachProbe Ilustración 31 puede extraer VISA, Master Card, American Express, JCB, Discover y tarjetas de crédito Diners Club a partir de archivos pcap.

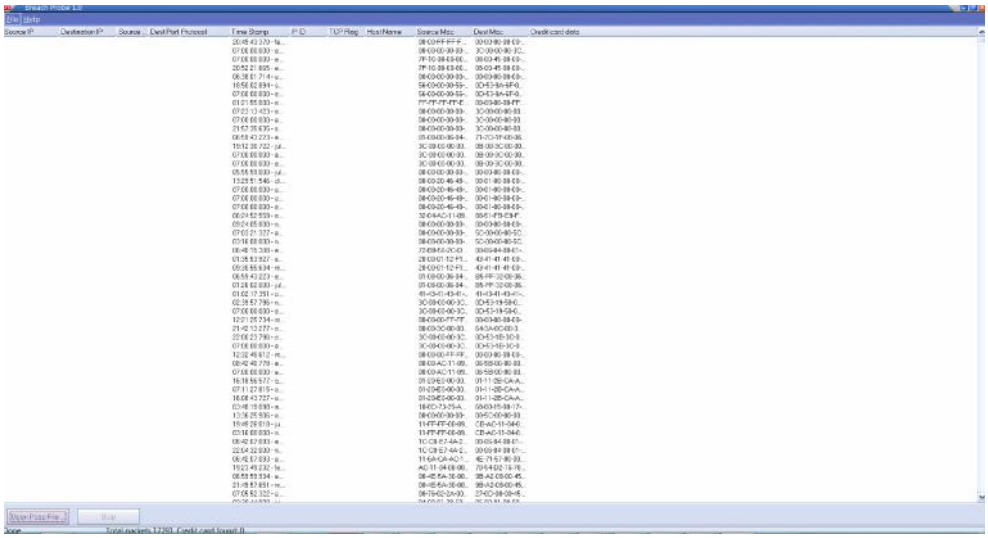


Ilustración 31 BreachProbe

Fuente: Software WireShark

Al no encontrar ningún resultado con esta herramienta ni mediante filtros a través del WireShark se analizó las características del switch, en el que se identificó que el mismo divide los paquetes en diferentes tramas, ya que cada paquete es transportado por la red de forma independiente de los otros, paquetes pertenecientes al mismo mensaje puede viajar por caminos diferentes, de tal manera que la capa de transporte reordena los datagramas y recupera los paquetes perdidos, por lo que de manera manual ni con la herramienta BreachProbe se lograría encontrar los datos de número de tarjetas.

Luego de analizar las características del switch se puso en consideración la herramienta CCSRCH ya que este software reconstruye las tramas que viajan a través de la red, dado que los datos de los titulares de las tarjetas de crédito van en varios segmentos lo que hace esta herramienta es agruparlos para exponer los datos completos de las tarjetas de crédito. Además se escogio esta herramienta ya que también permite examinar los archivos que esta con la extensión *.pcap.

CCSRCH

Se analizó la herramienta CCSRCH Ilustración 32 la cual es un software libre, y maneja las siguientes suposiciones dentro de la búsqueda de números de tarjeta de crédito:

1. Las tarjetas pueden ser de un mínimo de 14 números y un máximo de 16 números.
2. Números de tarjetas deben ser contiguos.
3. Los archivos se tratan como objetos binarios crudos y procesados.

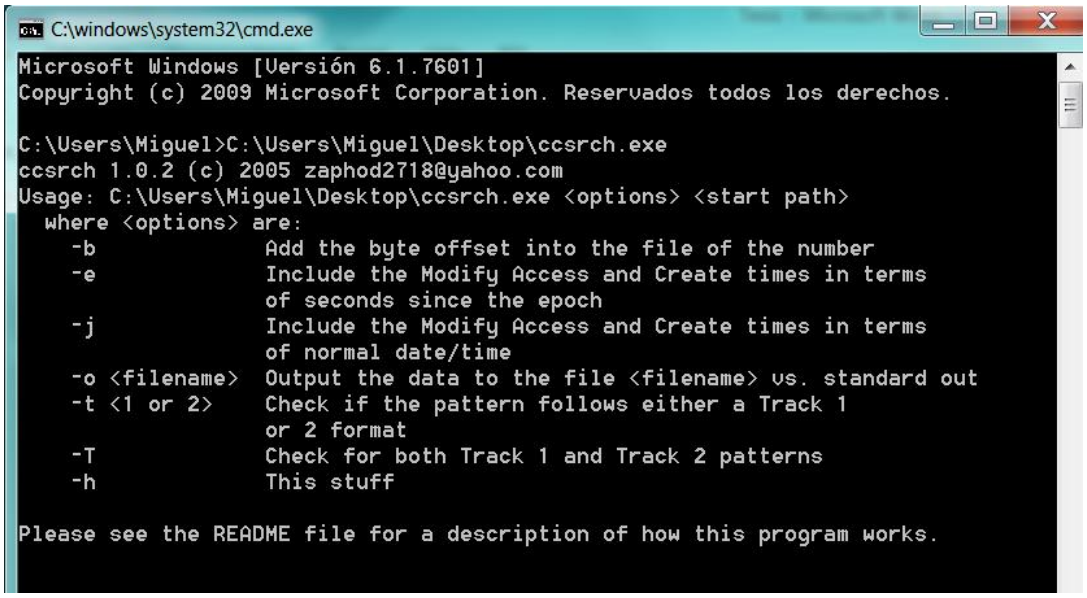


Ilustración 32 CCSRCH

Como ventajas de esta herramienta se puede decir lo siguiente:

- No requiere instalación
- Para sistemas operativos no soportados permite acceso al código y se puede compilar para la plataforma deseada
- Tasa media/baja de falsos positivos (detecta números repetidos en patrones p.e. 5454545454545454)
- Buena velocidad en la detección

- Permite perfilar las búsquedas en archivos con base en exclusión de determinadas extensiones
- Permite que en los resultados simplemente se muestre el nombre del archivo que contiene datos de tarjetas, para evitar extracción y almacenamiento de PAN y datos de bandas magnéticas durante la búsqueda siendo de mucha importancia en el manejo reservado de esta información.

Para lo cual a través de esta herramienta únicamente fue necesario dar el nombre del directorio y el archivo para que sea analizado y se encuentre números de tarjeta de crédito.

Es así que al analizar con esta herramienta los archivos obtenidos dentro del proceso de captura de datos se encontraron los resultados que se encuentran reflejados en las imágenes pero que por motivos de seguridad y de confidencialidad de los datos las imágenes se adulteraron las mismas para que el número de la tarjeta de crédito no sea legible por terceras personas dentro de este archivo, obteniendo los siguientes resultados:

En la captura de datos del nodo del Área de Contabilidad (punto 4) se encontró una tarjeta de crédito con número 4303********4333 el mismo que puede visualizarse en la Ilustración 33.

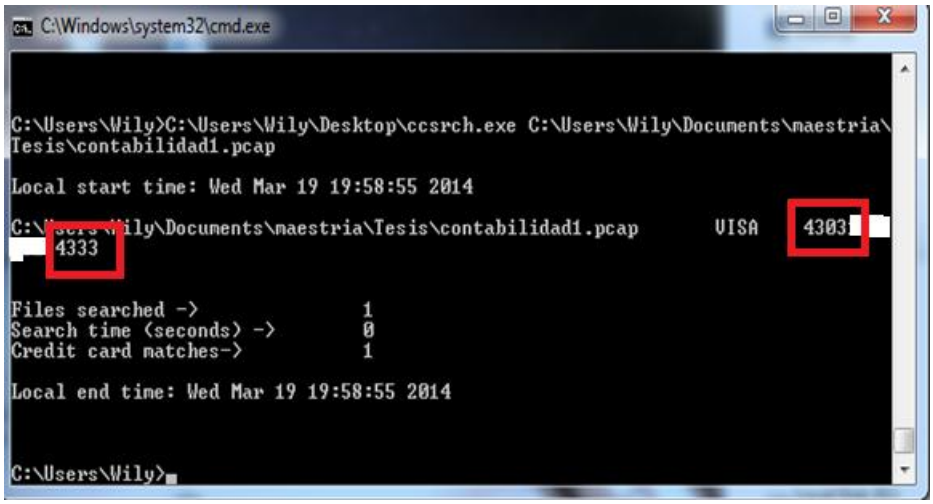
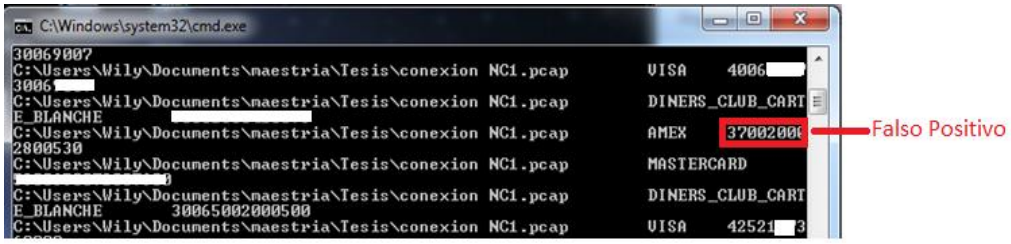


Ilustración 33 Contabilidad - CCSRCH Obtención Tarjetas de Crédito

En la captura de datos del nodo del Campus Matriz (punto 2) se encontró 1757 números de tarjeta de crédito como Visa, Diners y Mastercard (Ilustración 34), además se puede visualizar falsos positivos ya que la tarjeta American Express no es aceptada dentro de la Universidad (Ilustración 34).



En la captura del nodo de Tesorería (punto 6) se encontró dos números de tarjeta Diners Ilustración 35.

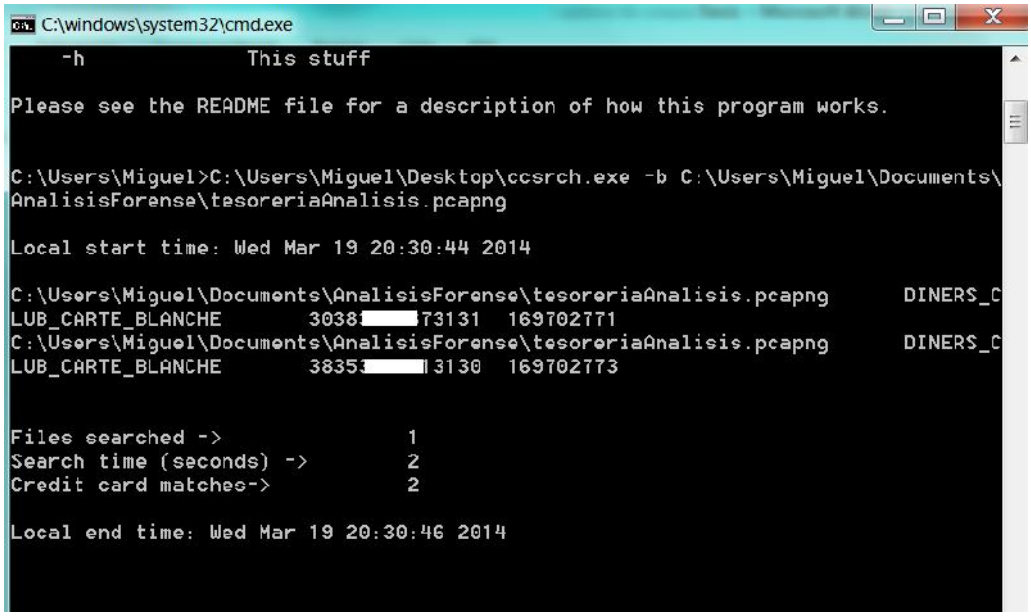


Ilustración 35 Tesorería - CCSRCH Obtención Tarjetas de Crédito

En el nodo del Campus UTE Occidental (punto 1) por motivos de seguridad se restringió el acceso y se pudo capturar por poco tiempo datos, por lo cual

dentro del análisis no se obtuvo ningún número de tarjeta de crédito Ilustración 36.

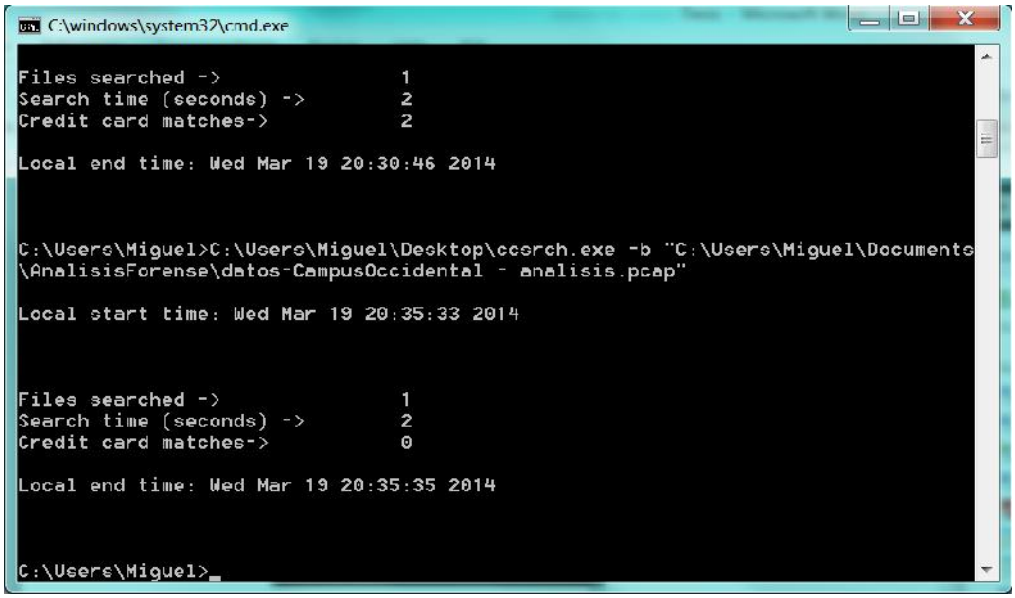


Ilustración 36 Campus Occidental - CCSRCH Obtención Tarjetas de Crédito

En resumen al analizar los datos a través de la herramienta CCSRCH se determinó que los datos de números de tarjeta de crédito pasan a través de la red sin ninguna encriptación.

4.2.6. Presentación

En esta etapa se describe las tareas realizadas que a modo de informe técnico se pone en conocimiento a las diferentes personas responsables en todo el proceso:

Informe Análisis Forense

Fecha: Quito, 15 de febrero de 2014

Atención: Universidad Tecnológica Equinoccial.

Autor del Informe: Ing. William Chumi, Ing. Daniel Flores.

Analistas Forenses

Antecedentes.

Por motivos de verificar la seguridad de los datos dentro de la Universidad Tecnológica Equinoccial se realiza un análisis a la red de la misma específicamente a las áreas de contabilidad, tesorería y sistemas, basados en la norma PCI-DSS la cual especifica la seguridad de datos referente a tarjetas de crédito y tarjetahabientes.

Con la presencia del Ing. Leonardo Arellano Analista Técnico de Infraestructura, se inicia la captura de datos de los puntos de red considerados dentro del análisis previo de la misma de la universidad realizado con el Ing. Javier Vivanco.

Trabajo Realizado.

Se procedió mediante entrevistas a verificar que datos de información referente a tarjetas de crédito que se almacena dentro del sistema de la universidad.

Mediante observación a la aplicación se verifica que el software SICAF dentro del módulo de tesorería almacena información relevante de tarjetas de crédito y del tarjeta habiente como el número de tarjeta el propietario y la autorización (Imagen Adjunta).

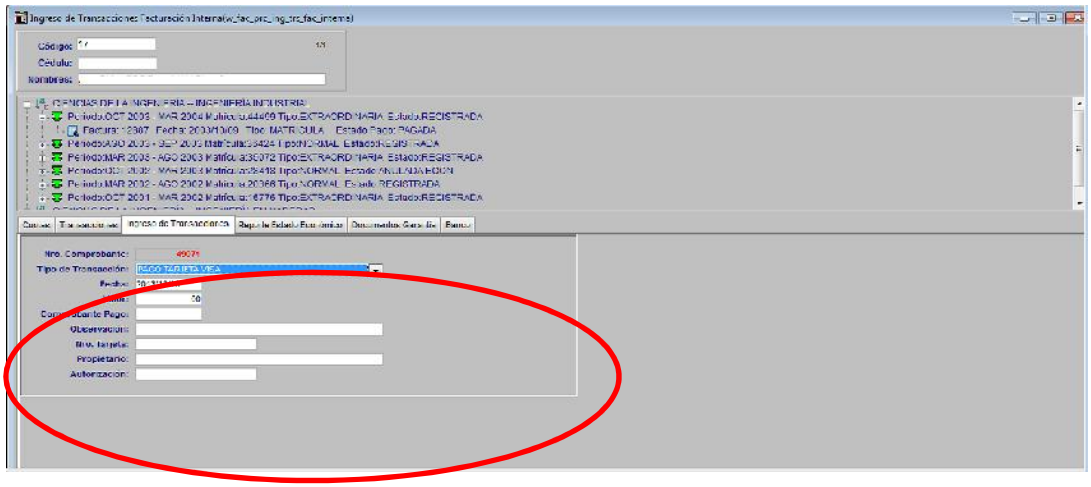
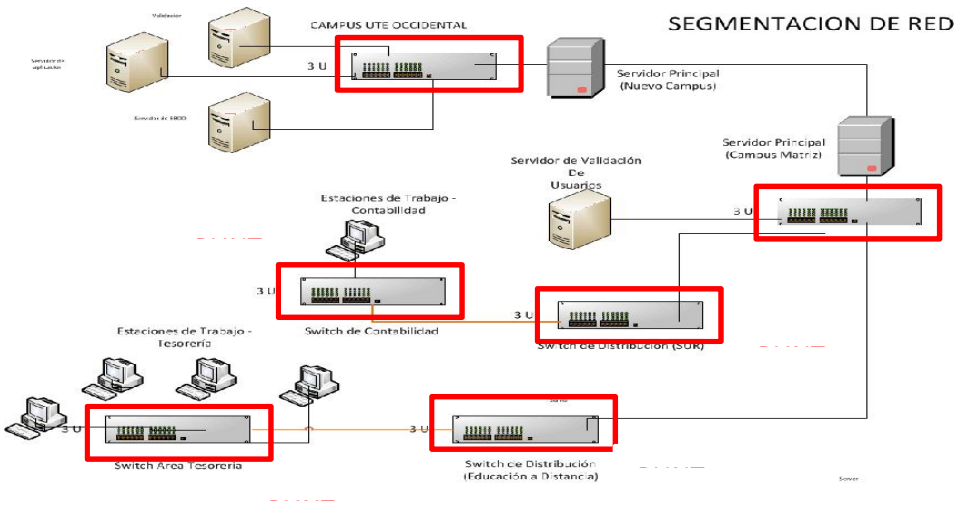


IMAGEN APLICATIVO SICAF DEPARTAMENTO DE TESORERIA

Además en el área de contabilidad mediante el sistema informático genera reportes, que mantienen de igual manera la información de tarjeta de crédito.

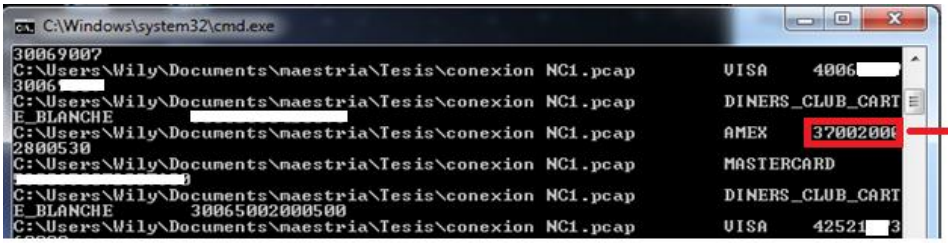
De tal manera que mediante la herramienta WireShark se captura los datos en diferentes puntos de red previamente analizados de acuerdo a las entrevistas y segmentación de la red, los mismos que se indican en la siguiente imagen.



Los puntos de la imagen son los siguientes:

- Punto 1 Switch Campus UTE Occidental
- Punto 2 Switch Principal Campus Matriz
- Punto 3 Switch de Distribución (Sur)
- Punto 4 Switch Área Contabilidad
- Punto 5 Switch de Distribución Educación a Distancia
- Punto 6 Switch Área Tesorería

Al realizar las entrevistas al Administrador de Redes, Administrador de la Aplicación y Administrador de Base de Datos de la Universidad supieron indicar que no se utiliza métodos de encriptación ni cifrado de datos. Para constatar lo antes expuesto, se utilizó diferentes herramientas como WireShark, BreachProbe y CCSRCH para realizar el análisis a los datos capturados, es así que mediante la herramienta CCSRCH se identificó números de tarjetas de crédito, por lo que se puede concluir que a través de la red de la Universidad se transmiten datos de tarjeta de crédito sin encriptar siendo esto una vulnerabilidad para la seguridad de datos de la institución.



Por tal razón la información que pudimos extraer son números de tarjetas de crédito y propietarios de las mismas.

Conclusiones.

1. De acuerdo a los requisitos 10 y 11 de la Norma PCI-DSS se indica que se debe supervisar y monitorear las redes con regularidad, además se debe probar con regularidad los

sistemas y procesos de seguridad. Se obtuvo captura de datos de la red de la Universidad mediante la herramienta idónea para esta tarea como es WireShark.

2. Mediante la utilización de herramientas de análisis forense como:
   - WireShark
   - BreachProbe
   - CCSRCH

   Se evidencio que a través de la red de la institución los datos se trasmiten sin ningún tipo de cifrado ni encriptación.

   Por lo que concluye que la Universidad no cumple con la norma ya que los datos de número de tarjetas de crédito y la información relacionada con la misma deben quedar protegidos. Esta protección debe brindarse por cada requisito de las PCI-DSS, a fin de asegurar una protección integral del entorno del titular de la tarjeta.

Atentamente

Ing. William Chumi Ing. Daniel Flores

CAPITULO V

5.1. Plan de Acción

En este capítulo se pone a consideración las tareas recurrentes que recomienda la Norma PCI-DSS y un plan de acción en base a los requisitos 10 y 11 de la norma como aporte para la Universidad que está en el derecho de acatar o no las mimas, pero que generan un plus adicional dentro de las instituciones de su categoría ya que cumple con la protección de los datos de las tarjetas de crédito

En el desempeño de las actividades, la Universidad Tecnológica Equinoccial almacena, procesa y transmite datos de tarjetas. Este hecho conlleva la obligación de cumplir con las medidas de protección de la información de titulares de tarjetas acordadas por las marcas y reflejadas en el Payment Card Industry Data Security Standard (PCI DSS).

Para el proceso de la implementación de los requisitos 10 y 11 de la Norma PCI DSS se han identificado básicamente dos etapas.

5.1.1. Primera Etapa: Análisis de Requisitos

Donde se realiza el análisis de todos los requerimientos (12 en total) de acuerdo a la Ilustración 37, para ubicar a la Universidad Tecnológica Equinoccial en cuales requerimientos ya se encuentran alineados al estándar del PCI DSS, como resultado de su trabajo diario y cuales requerimientos no están alineados, para generar planes de acción que le permitan a la Universidad completar de forma satisfactoria con los 12 requerimientos.

Normas de seguridad de datos de la PCI: descripción general de alto nivel

Crear y mantener una red segura	
Requisito 1:	Instale y mantenga una configuración de firewall para proteger los datos de los titulares de las tarjetas
Requisito 2:	No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores
Proteja los datos del titular de la tarjeta	
Requisito 3:	Proteja los datos del titular de la tarjeta que fueron almacenados
Requisito 4:	Codifique la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas
Desarrolle un programa de administración de vulnerabilidad	
Requisito 5:	Utilice un software antivirus y actualícelo regularmente
Requisito 6:	Desarrolle y mantenga sistemas y aplicaciones seguras
Implemente medidas sólidas de control de acceso	
Requisito 7:	Restrinja el acceso a los datos de los titulares de las tarjetas conforme a la necesidad de conocer de la empresa
Requisito 8:	Asigne una ID exclusiva para cada persona que tenga acceso al sistema informático
Requisito 9:	Limite el acceso físico a los datos del titular de la tarjeta
Supervise y pruebe las redes regularmente	
Requisito 10:	Rastree y supervise los accesos a los recursos de red y a los datos de los titulares de las tarjetas
Requisito 11:	Pruebe los sistemas y procesos de seguridad regularmente
Mantenga una política de seguridad de información	
Requisito 12:	Mantenga una política que aborde la seguridad de la información

Ilustración 37 Requisitos Norma PCI-DSS

Fuente: Normas de Seguridad de Pago

5.1.2. Segunda Etapa: Plan de Cumplimiento

Es la puesta en marcha de los planes de acción y la ejecución de auditorías internas para garantizar de forma definitiva, que dentro de la Universidad se encuentra implementado los requisitos 10 y 11 que involucran dentro de su gestión diaria.

5.1.2.1. Consideración:

El presente proyecto contempla solo la primera etapa del proceso de certificación del PCI DSS, es decir, la etapa de análisis, basados en un modelo de implantación y adopción en el proceso de mejora continua para un entorno PCI DSS en el cual se requiere de una planificación y preparación previa, la ejecución de las acciones identificadas (implementación de controles y requerimientos del estándar), la validación de la efectividad y eficacia de dichos resultados (realización de una auditoría o de un ejercicio de autoevaluación) y un aprendizaje continuo dentro de un ciclo anual. La idea detrás del uso de esta metodología es

la de definir una estrategia que permita mantener y optimizar en cada iteración los niveles de seguridad de la información requeridos por el estándar a lo largo del tiempo, que está a consideración de la Universidad implementar o no.

5.1.2.2. Beneficios a Lograr:

Como beneficios se espera:

- Contemplar un nivel de seguridad de la información, haciendo a la Universidad más segura en cuanto a las transacciones financieras que se realice con tarjeta de crédito además para el desarrollo de los diferentes proyectos informáticos.
- Por otra parte, se convierte en una ventaja competitiva, donde la seguridad de información confidencial es primordial.

5.1.3. Recomendaciones generales para la aplicación de controles de PCI-DSS, orientados al monitoreo y gestión de eventos.

El estándar PCI-DSS contempla una serie de acciones físicas, técnicas y administrativas a ser desarrolladas en determinados periodos de tiempo con el fin de garantizar que los controles que se van a implementar o han sido implementados cumplen de forma idónea, eficiente y eficaz con la intención del requerimiento asociado. De esta manera se puede identificar de forma anticipada cualquier desviación y actuar de forma oportuna, minimizando la posibilidad de errores en la operación, de tal manera se identificó como recomendaciones los siguientes puntos descritos.

Dada la complejidad inicial que se presenta frente a la implementación de una infraestructura de monitoreo y gestión de eventos, además de las pruebas que regularmente se debe realizar como indican los requisitos 10 y 11 en una organización que procese, almacene o transmita datos de tarjetas, es necesario establecer un modelo metodológico que permita orientar el trabajo hacia la optimización de recursos y tiempos, con base en las necesidades detectadas. Para ello, es importante enfocarse en las siguientes labores:

1. Unificar controles en los cuales se tiene un cumplimiento parcial o total: primordialmente se debe identificar los elementos que se encuentran actualmente en la infraestructura como son routers, switchs puntos de acceso, dispositivos de red identificados de acuerdo a la segmentación de la red realizada en las área que se encuentran involucradas en el proceso y transmisión de datos de tarjeta de crédito como son Tesorería, Contabilidad y Sistemas , y que para cumplir con la norma PCI-DSS pueden ser reutilizados o reconfigurados. De igual manera, se debe plantear los mismos cuestionamientos en términos de procesos y recursos, con la finalidad de no incurrir en gastos y esfuerzos innecesarios.
2. Definir e identificar a las personas que acceden a la información: Es importante segregar funciones y roles y definir restricciones de acuerdo a los perfiles identificados, con esto se reduce problemas de privilegios, además ayuda a la detección de errores involuntarios, fraudes y ocultamiento de rastros, es así que en el área de tesorería y contabilidad los roles de cada funcionario deben ser muy precisas para el manejo de la información de tarjetas de crédito, dentro del área de sistemas de la Universidad se debe identificar que personas pueden acceder a la información almacenada y quien administrar los servidores que alojan esta información.
3. Establecer funciones técnicas para la configuración de logs en servidores, aplicaciones, red y seguridad perimetral: todos los elementos presentes en la red son diferentes, generan diferentes tipos de eventos y los formatos de registro de eventos son múltiples. Es necesario definir estrategias de tipo técnico para configurar cada elemento conforme con los requerimientos de PCI-DSS. Para ello, se puede apoyar la labor en la definición de procedimientos de configuración y/o guías de aseguramiento y listas de validación.
4. Definir y contemplar los recursos requeridos para el almacenamiento: Los tamaños de los archivos de registro y monitoreo son directamente proporcionales a la cantidad de eventos generados y servicios/servidores gestionadores. Por ello, con la ayuda de los administradores de Red, Aplicativos, y de Base de Datos de la Universidad estimar un espacio de

almacenamiento en local de dichos registros, de por lo menos tres meses. Para presupuestar las necesidades, se recomienda utilizar varios servidores representativos (por sistema operativo o por función) como pilotos, hacer un seguimiento estadístico por hora/día/semana el uso de disco y extrapolar dichos resultados en la totalidad de elementos técnicos del entorno. Teniendo en cuenta que es obligatorio el uso de un servidor centralizado de registros, dicho servidor debe tener espacio suficiente en disco, para almacenar los archivos de eventos de todos los equipos del entorno durante el tiempo estipulado (3 meses), además de contar con una estrategia de respaldo (backup) que permita mantenerlos durante un año.

Así mismo, se debe tener en cuenta recomendaciones generales de seguridad en almacenamiento de registros:

- Definición de un disco/partición/sistema de archivos (Filesystem) independiente para el almacenamiento en local.
- Aplicación de controles de acceso y permisos. Se recomienda emplear características y funcionalidades propias de los sistemas de archivos, como restricciones de ejecución de binarios, controles de inmutabilidad, permisos de "solo agregación" en archivos (append-only) y controles para evitar el borrado.
- Activar funcionalidades como "registro cíclico" por tiempo, no por tamaño, Esto permitirá que después de un tiempo específico, los eventos más recientes sobrescriban a los más antiguos de forma circular en el mismo archivo.

5. Identificar el impacto en la eficacia de los servicios y servidores causados por la generación de logs: para identificar dicho impacto de los servicios y servidores se debe basar en la estructura de la base de datos y de la red dentro del departamento de sistemas de la universidad debido a que la generación de registros de eventos consume recursos del sistema (memoria intermedia, uso de procesador, uso de recursos de I/O), y con la ayuda del personal técnico de la Institución se debe contemplar el impacto que tiene dicho consumo sobre la capacidad general del servidor y los servicios asociados.
6. Determinar métodos de análisis de logs: después de tener activados y almacenados correctamente los archivos de registro de eventos dentro del

departamento de sistemas de la Universidad, es necesario definir una estrategia de análisis y correlación de información, que permita obtener datos específicos frente a una acción en concreto haciendo más fácil para el área de sistemas determinar el análisis de los logs. Dependiendo de la complejidad del entorno, miles de registro de eventos son generados por todos los elementos monitorizados, haciendo inmanejable la ubicación de un dato concreto.

7. Establecer criterios para considerar a un evento como un incidente y su impacto relacionado: Dentro del departamento de sistemas de la Universidad se puede generar un historial o un reporte de todos los eventos generados como incidente con su impacto respectivo en donde se debe, fijar una serie de alertas, establecimiento de tiempos en los cuales dichas alertar deben ser atendidas y los procesos asociados. Todo ello en función de la criticidad y del impacto que el evento pueda tener en la confidencialidad e integridad de los datos relacionados con PCI-DSS.
8. Aplicar controles orientados al aseguramiento de los registros de eventos: Con el fin de garantizar la idoneidad e integridad de los archivos de registros de eventos, es imprescindible implementar controles que permitan la identificación de eventos sospechosos durante la manipulación de dichos archivos, tales como modificación intencional, no intencional, extracción de información, cambio de permisos y/o propietarios, borrado total o parcial y agregación. En este sentido, el requerimiento se orienta hacia la instalación de un sistema de monitorización de integridad o detección de cambios. Es así que se debe aplicar el control expuesto en la norma que es la segregación de funciones y la asignación de roles para el acceso a los servidores de la Institución.
9. La forma más robusta de prevención de intrusiones: el departamento de sistemas de la universidad está encargada de asegurarse que todas las comunicaciones entrantes y salientes del sistema de los departamentos de tesorería y contabilidad sean mutuamente autenticadas para controlar efectivamente el acceso de la información de los titulares de tarjeta de crédito a través del aplicativo SICAF que maneja la Universidad.

10. Evaluar qué tipo de herramientas pueden ser útiles, bajo que conceptos y su ámbito de acción: para el cumplimiento de los controles se requiere implementar un sistema centralizado de registros para lo cual se puede utilizar diferentes herramientas que almacenan registros de aplicación, de seguridad y registros del sistema la cual puede ser monitoreada por el Administrador de Red o de Aplicativo con la finalidad de que sea alertado en el caso de falla, además se debe utilizar software de sincronización de tiempos y software de recolección, análisis y generación de alertas. Dependiendo de la complejidad del entorno afectado por el cumplimiento de PCI-DSS, la cantidad de elementos involucrados y el número promedio de eventos generados en umbrales de tiempo predefinidos (minutos, horas, días) y el personal y recursos disponibles, se puede optar por el uso de software OpenSource, herramientas comerciales o una mezcla de ambas, siempre bajo el concepto costo-beneficio.
11. Definir prioridades en la implementación de controles globales: debido a la alta interacción e interdependencia entre todos los controles del estándar, se deben identificar a nivel general, aquellas acciones que preceden a otras, para no duplicar el trabajo. En este sentido, PCI-DSS publicó una guía el cual sirve al departamento de sistemas de la Universidad en la definición de hitos organizados de acuerdo con la prioridad de implementación. Cada hito abarca una serie de controles y son presentados a manera de recomendación, ya que cada organización puede definir sus propias prioridades conforme con el escenario de cumplimiento. Dichos hitos son:
    i. Remover datos sensitivos y limitar los periodos de retención.
    ii. Proteger las redes perimetrales, internas e inalámbricas.
    iii. Asegurar las aplicaciones de pago con tarjetas.
    iv. Monitorear y controlar el acceso a los sistemas.
    v. Proteger los datos de los tarjetahabientes almacenados.
    vi. Finalizar las tareas restantes de cumplimiento y asegurarse que los controles están implementados satisfactoriamente.

En el proceso de implementación de la plataforma de monitorización viene posterior al desarrollo de proyectos de aseguramiento, redes y aplicaciones por lo

que es primordial identificar cuándo se deben aplicar estos controles para no incurrir en errores.

Además de la implementación de los requerimientos expuestos a modo de recomendación para la implementación de toda la norma se debería verificar que las tareas periódicas (o "tareas recurrentes") hayan sido ejecutadas y se tenga evidencia de dicha ejecución (registros, resultados, formularios, diagramas, etc.) ya que la ausencia de evidencia de una de estas tareas puede conllevar al incumplimiento de un requerimiento.

Es así que a continuación se presenta un resumen de las diferentes tareas recurrentes presentes en el estándar PCI DSS. Este listado ha sido desarrollado para facilitar a la universidad y coordinación de labores y prevenir que por olvido alguna tarea no sea ejecutada dentro de los umbrales temporales definidos.

Req. PCI DSS	Descripción	Periodicidad
1.1.2	Actualización del diagrama de red	Cada cambio significativo
1.1.3	Actualización del diagrama de flujo de datos de tarjetas	Cada cambio significativo
1.1.7	Revisión de reglas de switchs y routers	Semestral
2.5	Validación de aplicación de políticas de seguridad y procedimientos operativos para la gestión de cambios en valores por defecto y otros parámetros de seguridad	Continuamente
3.1.a	Proceso para eliminar datos de tarjeta almacenados fuera del umbral de retención	Trimestral
3.6.4.a	Cambio de claves de cifrado	Criptoperiodo
3.6.5.a	Retiro o remplazo de claves de cifrado	A la salida de un empleado que conozca la clave o cuando se sospeche que la clave está en riesgo
3.7	Validación de aplicación de políticas de seguridad y procedimientos operativos para la protección de datos de tarjeta almacenados	Continuamente
4.3	Validación de aplicación de políticas de seguridad y	Continuamente

CONTINUA

	procedimientos operativos para la encriptación de transmisiones de datos de tarjeta	
5.2.b	Ejecución de escaneos anti-virus y actualizaciones automáticas	Periódicamente (La periodicidad debe ser definida por la organización)
6.1	Identificación y catálogo de nuevas vulnerabilidades	Continuamente
6.3.1	Eliminación de cuentas, ID de usuario y contraseñas en aplicaciones desarrolladas	Antes de ingreso a producción
6.3.2	Revisión de código personalizado	Antes de ingreso a producción
6.5.a	Formación en técnicas de codificación segura para desarrolladores	Periódicamente (La periodicidad debe ser definida por la organización)
6.6	Evaluación de vulnerabilidades en aplicaciones (aplica si no se usa un WAF)	Anual Cada cambio significativo
6.7	Validación de aplicación de políticas de seguridad y procedimientos operativos para el desarrollo y mantenimiento de sistemas seguros y aplicaciones	Continuamente
7.3	Validación de aplicación de políticas de seguridad y procedimientos operativos para la restricción de acceso a datos de tarjeta	Continuamente
9.5.1.b	Revisión de las ubicaciones de almacenamiento de medios de copias de seguridad	Anual
9.8	Destrucción de medios que contengan datos de tarjetas	Cuando ya no sean necesarios
9.10	Validación de aplicación de políticas de seguridad y procedimientos operativos para la restricción de acceso físico a datos de tarjetas de pago	Continuamente
10.5.3	Realización de copias de seguridad de pistas de auditoría en un servidor central	Inmediato

CONTINUA

10.6.1	Revisión de los registros de auditoría (logs)	**PCI DSS v2.0:** Diario **PCI DSS v3.0:** Diario de los siguientes elementos: - Todos los eventos de seguridad - Logs de todos los componentes de sistemas que almacenan, procesan y/o transmiten datos de tarjeta y/o datos sensibles de autenticación (SAD) o que puedan impactar la seguridad de dichos datos - Logs de todos los componentes de sistema críticos - Logos de todos los servidores y componentes de sistemas que ejecuten funciones de seguridad
10.6.2	Revisión de los registros de auditoría (logs) de otros componentes del sistema	Con base en la política de la organización y estrategia de gestión de riesgos
10.7	Conservación del historial de pistas de auditoría	Trimestral (disponible) Anual
10.8	Validación de aplicación de políticas de seguridad y procedimientos operativos para la monitorización de todos los accesos a recursos de red y datos de tarjeta de pago	Continuamente
11.2.1	Realización de análisis de vulnerabilidades internas	Trimestral
11.2.2	Realización de análisis de vulnerabilidades externas (ASV)	Trimestral
11.2.3	Realización de análisis de vulnerabilidades interno y externo	Cada cambio significativo
	Pruebas de penetración externas e internas a nivel de capa de red y capa de aplicación	Anual Cada cambio significativo
11.3.1	Pruebas de penetración externas	Anual Cada cambio significativo

CONTINUA

11.3.2	Pruebas de penetración internas	Anual Cada cambio significativo
11.3.4	Ejecución de pruebas de penetración en el caso que se use segmentación para aislar el CDE de otras redes	Anual Cada cambio significativo
11.4.c	Actualización de IDS/IPS (motores, líneas base y firmas)	Continuamente
11.5.b	Comparación de archivos críticos (FIM)	Semanalmente
11.6	Validación de aplicación de políticas de seguridad y procedimientos operativos para la monitorización de seguridad y pruebas	Continuamente
12.2	Ejecución de un proceso que identifique las amenazas, vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Anual
12.1.1	Revisión de la política de seguridad de la información	Anual Cada cambio significativo
	Ejecución de los procedimientos de seguridad operativa	Diario
12.10.2	Prueba del plan de Respuesta a Incidentes	Anualmente
12.10.4	Formación adecuada al personal en responsabilidades de respuesta ante fallos de seguridad	Periódicamente (No se indica periodicidad específica)

5.1.4. Propuesta en Base a Análisis

Además de las tareas recurrentes que aconseja la norma PCI-DSS que deben ser validadas por parte de la Universidad, es importante ejecutar el siguiente plan de acciones que queda a potestad de la Universidad la implementación, que fue desarrollado acorde a las funciones que se desempeñan dentro la Universidad con respecto al manejo de la información de las tarjetas de crédito, por ese motivo se propone a modo de proyectos para el cumplimiento de los Requisitos 10 y 11 de la Norma PCI-DSS que indica que se debe monitorear y probar las redes así como sistemas y procesos de seguridad regularmente ya que la importancia de estos requisitos se fundamente en contar con una buena gestión de eventos y registros que permitirán prevenir, detectar, corregir y evaluar cualquier amenaza que afecte

a la integridad, confidencialidad y disponibilidad de los datos relacionados con tarjetas de crédito que soporten cualquier procedimiento investigativo y/o actividades relacionadas posterior a un incidente y que sirvan para implementar políticas de seguridad de la información.

Tabla 4 Proyecto 1 para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información.

PROYECTO: Proteger los datos del titular de la tarjeta	
RESPONSABLE: Por Asignar por parte de la Universidad	
REQUERIMIENTO CUBIERTO	FECHA LIMITE
1.- Almacenar la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos. **2.- No almacenar datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados).** **3.- Oculte el PAN (Número de cuenta principal) cuando aparezca (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá).** **4.- Verificar que el PAN quede ilegible en cualquier lugar donde se almacene (incluidos los datos que se almacenen en medios digitales portátiles, en medios de copia de seguridad y en registros) utilizando cualquiera de los siguientes métodos:** ***Valores hash de una vía basados en criptografía sólida (el hash debe ser de todo el PAN).** ***Truncamiento (los valores hash no se pueden usar para reemplazar el segmento truncado del PAN)** ***Tokens y ensambladores de índices (los ensambladores se deben almacenar de manera segura).** ***Sólida criptografía con procesos y procedimientos de gestión de claves relacionadas.**	
TAREAS	
1.- Verificar que las políticas y los procedimientos incluyan todo el almacenamiento de datos de titulares de tarjetas. **2.- Verificar que las políticas y los procedimientos incluyan por lo menos una de las siguientes:** ***Un proceso programático (automático o manual) para eliminar, por lo menos trimestral, datos de titulares de tarjetas almacenados que excedan los requisitos definidos en la política de retención de datos** ***Requisitos para una revisión, la cual se debe realizar por lo menos trimestralmente, para verificar que los datos de titulares de tarjetas almacenados no excedan los requisitos definidos en la política de retención de datos.** **3.- En el caso de una muestra de componentes del sistema que almacenan datos de titulares de tarjetas, verificar que los datos almacenados no excedan los requisitos definidos en la política de retención de datos**	

CONTINUA

4.- En el caso de la muestra de componentes del sistema, examinar las fuentes de datos, incluido, a modo de ejemplo, lo siguiente y verificar que el contenido completo de cualquier pista de la banda magnética en el reverso de la tarjeta o cualesquiera datos almacenados en un chip no se almacenen bajo ninguna circunstancia:

***Datos de transacciones entrantes**

***Todos los registros (por ejemplo, transacciones, historiales, depuración, error)**

***Archivos de historial**

***Archivos de seguimiento**

***Esquemas de bases de datos**

***Contenidos de bases de datos**

5.- En el caso de la muestra de componentes del sistema, examinar las fuentes de datos y verificar, incluyendo, pero sin limitarse a, que el código o el valor de verificación de la tarjeta de tres dígitos o de cuatro dígitos impreso en el anverso de la tarjeta o en el panel de firma (datos CVV2, CVC2, CID, CAV2) no quede almacenado bajo ninguna circunstancia:

***Datos de transacciones entrantes**

***Todos los registros (por ejemplo, transacciones, historiales, depuración, error)**

***Archivos de historial**

***Archivos de seguimiento**

***Esquemas de bases de datos**

***Contenidos de bases de datos**

6.- En el caso de la muestra de componentes del sistema, evaluar las fuentes de datos y evalúe, incluyendo, pero sin limitarse a, que los PIN y los bloqueos de PIN cifrados no se almacenen en ninguna circunstancia:

***Datos de transacciones entrantes**

***Todos los registros (por ejemplo, transacciones, historiales, depuración, error)**

***Archivos de historial**

***Archivos de seguimiento**

***Esquemas de bases de datos**

***Contenidos de bases de datos**

7.- Obtener y evaluar las políticas escritas y revisar las vistas de PAN (por ejemplo, en la pantalla, en recibos en papel) a fin de controlar que los números de las cuentas principales (PAN) se ocultan al visualizar los datos de los titulares de las tarjetas, excepto en los casos en que existe una necesidad comercial legítima de visualizar el PAN completo

8.- Verificar que las claves criptográficas estén almacenadas de forma segura (por ejemplo, se almacenen en medios portátiles protegidos adecuadamente con controles sólidos de acceso).

9.- Verificar que los datos de los titulares de las tarjetas almacenados en medios portátiles se cifren donde quiera que se almacenen

Tabla 5 Proyecto 2 Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas

PROYECTO: Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas
RESPONSABLE: Por Asignar por parte de la Universidad
REQUERIMIENTO CUBIERTO FECHA LIMITE
1.- Nunca debe enviar PAN no cifrados por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea, el chat, etc.).
TAREAS
1.-Verificar que el PAN quede ilegible o asegurado con cifrado sólido cada vez que se envíe mediante tecnologías de mensajería de usuario final **2.- Verificar la existencia de una política que establezca que los PNA no cifrados no se deben enviar por medio de tecnologías de mensajería de usuario final**

Tabla 6 Proyecto 3 Desarrolle y mantenga sistemas y aplicaciones seguras

PROYECTO: Desarrolle y mantenga sistemas y aplicaciones seguras
RESPONSABLE: Por Asignar por parte de la Universidad
REQUERIMIENTO CUBIERTO FECHA LIMITE
1.- Desarrollo de aplicaciones de software (acceso interno y externo, e incluso acceso administrativo basado en la web a aplicaciones) de conformidad con las PCI DSS (por ejemplo, **autenticación segura y registro), basadas en las mejores prácticas de la industria. Incorpore seguridad de la información en todo el ciclo de vida de desarrollo del software.** **2.- Seguir los procesos y procedimientos de control de todos los cambios en los componentes del sistema** **3.- Desarrollar aplicaciones basadas en directrices de codificación seguras. Evite vulnerabilidades de codificación comunes en los procesos de desarrollo de software**
TAREAS
1.- Obtener y analizar las políticas para confirmar que todos los cambios a los códigos de aplicaciones personalizadas de se deban revisar (ya sea mediante procesos manuales o automáticos) de la siguiente manera: *** Los cambios a los códigos son revisados por individuos distintos al autor que originó el código y por individuos con conocimiento en técnicas de revisión de código y prácticas de codificación segura.** *** Las revisiones de los códigos aseguran que estos se desarrollan de acuerdo con las directrices de codificación segura (consulte el requisito 6.5 de las PCI DSS).** ***Las correcciones pertinentes se implementan antes del lanzamiento.** ***La gerencia revisa y aprueba los resultados de la revisión de códigos antes del lanzamiento.** **2.- Los entornos de prueba/desarrollo están separados del entorno de producción y se implementa un control del acceso para reforzar la separación.**

CONTINUA

3.- Existe una separación de funciones entre el personal asignado a los entornos de desarrollo/prueba y los asignados al entorno de producción.

4.- Los datos de producción (PAN activos) no se utilizan para las pruebas ni para el desarrollo.

5.- Los datos y las cuentas de prueba se eliminan antes de que se active el sistema de producción.

6.- Verificar que los procedimientos de control de cambio relacionados con la implementación de los parches de seguridad y las modificaciones de software estén documentado

7.- En el caso de la muestra de componentes de sistema y cambios o parches de seguridad recientes, realizar un seguimiento de los cambios relacionados con la documentación de control de cambios. Por cada cambio que examine, realice lo siguiente:

8.- Verificar que la documentación que tiene incidencia se incluya en la documentación de control de cambios de cada cambio.

9.- Verificar que la aprobación documentada por partes autorizadas esté presente para cada muestra de cambio.

10.- Para cada cambio probado, verificar que la prueba de funcionalidad se haya realizado para verificar que el cambio no incide de forma adversa en la seguridad del sistema.

11.- En el caso de cambios del código personalizado, verificar que se hayan realizado las pruebas a todas las actualizaciones de conformidad antes de su implementación para producción.

12.- Verificar que se prepare los procedimientos de desinstalación para cada cambio.

13.- Obtener y revisar los procesos de desarrollo de software. Verificar que el proceso requiera capacitación acerca de las técnicas de codificación segura para desarrolladores, que esté basada en las mejores prácticas de la industria, así como asesoría.

14.- Entrevistar a un grupo modelo de desarrolladores y obtener pruebas de que son expertos en técnicas de codificación segura.

15.- Verificar que existan procesos implementados para garantizar que las aplicaciones no son vulnerables, como mínimo, a lo siguiente:

16.- Errores de inyección, en especial, errores de inyección SQL. (Valide la entrada para verificar que los datos de usuario no pueden modificar el significado de los comandos y las consultas, utilice las consultas basadas en parámetros, etc.).

17.- Desbordamiento de buffer (validar límites del buffer y truncar cadenas de entrada).

18.- Almacenamiento cifrado inseguro (prevenir defectos de cifrado).

19.- Comunicaciones inseguras (cifrar adecuadamente todas las comunicaciones autenticadas y confidenciales).

20.- Manejo inadecuado de errores (no permitir que se filtre información a través de mensajes de error)

21.- Todas las vulnerabilidades —altas‖ identificadas en el Requisito 6.2 de las PCI DS

22.- Lenguaje de comandos entre distinto sitios (XSS) (valide todos los parámetros antes de la inclusión, utilice técnicas de escape sensibles al contexto, etc.).

23.- Control de acceso inapropiado tal como referencias no seguras a objetos directos, no

CONTINUA

restricción de acceso a URL y exposición completa de los directorios (Autentique usuarios de forma correcta y desinfecte entradas. No exponga referencias a objetos internos a usuarios). **24.- Falsificación de solicitudes entre distintos sitios (CSRF). (No confíe en las credenciales de autorización ni en los tokens que los exploradores presentan automáticamente).**

Tabla 7 Proyecto 4 Asignar una ID exclusiva a cada persona que tenga acceso por computadora

PROYECTO: Asignar una ID exclusiva a cada persona que tenga acceso por computadora	
RESPONSABLE: Por Asignar por parte de la Universidad	
REQUERIMIENTO CUBIERTO	FECHA LIMITE
1.- Asignar a todos los usuarios una ID única antes de permitirles tener acceso a componentes del sistema o a datos de titulares de tarjetas. **2.- Además de la asignación de una ID única, emplear al menos uno de los métodos siguientes para autenticar a todos los usuarios:** *** Algo que el usuario sepa, como una contraseña o frase de seguridad** *** Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente** *** Algo que el usuario sea, como un rasgo biométrico**	
TAREAS	
1.- Verificar que todos los usuarios tengan asignada una ID única para tener acceso a componentes del sistema o titulares de tarjetas. **2.- Para verificar que los usuarios se autentiquen con una ID única y una autenticación adicional (por ejemplo, una contraseña) para tener acceso al entorno de datos de titulares de tarjetas, realizar lo siguiente:** *** Obtener y examinar la documentación que describe los métodos de autenticación utilizados.** *** Para cada tipo de método de autenticación utilizado y para cada tipo de componente del sistema, observar una autenticación para verificar que funcione de forma coherente con los métodos de autenticación documentado**	

Tabla 8 Proyecto 5 Restringir el acceso físico a los datos del titular de la tarjeta

PROYECTO: Restringir el acceso físico a los datos del titular de la tarjeta	
RESPONSABLE: Por Asignar por parte de la Universidad	
REQUERIMIENTO CUBIERTO	FECHA LIMITE
1.- Restringir el acceso físico a conexiones de red de acceso público. Por ejemplo, las áreas que sean accesibles a los visitantes no deben tener puertos de red habilitados a menos que se autorice explícitamente el acceso a la red. **2.- Limitar el acceso físico a los puntos de acceso inalámbricos, gateways, dispositivos**	

CONTINUA

manuales, hardware de redes/comunicaciones y líneas de telecomunicaciones. **3.- Enviar los medios por correo seguro u otro método de envío que se pueda rastrear con precisión.**
TAREAS
1.- Verificar que sólo empleados autorizados habiliten las conexiones de red en sitio sólo cuando sea necesario realizando entrevistas y observando. De forma alternativa, verificar que los visitantes estén acompañados en todo momento en áreas con conexiones de red activas. **2.- Verificar que el acceso físico a los puntos de acceso inalámbricos, gateways, dispositivos manuales, hardware de redes/comunicaciones y líneas de telecomunicaciones haya sido correctamente limitado.** **3.- Verificar que todos los medios enviados fuera de la empresa esté registrado y cuente con la autorización de la gerencia, así como también que se envíe por correo seguro u otro método de envío que se pueda rastrear.**

Tabla 9 Proyecto 6 Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas

PROYECTO: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas	
RESPONSABLE: Por Asignar por parte de la Universidad	
REQUERIMIENTO CUBIERTO	FECHA LIMITE
1.- Implementar pistas de auditoría automatizadas para todos los componentes del sistema a fin de reconstruir los eventos **2.- Registrar al menos las siguientes entradas de pistas de auditoría de los componentes del sistema para cada evento:** *** Utilizando tecnología de sincronización, sincronizar 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 Protocolo de tiempo de la red (Network Time Protocol (NTP)** **3.- Conservar el historial de pista de auditorías durante al menos un año, con un mínimo de tres meses inmediatamente disponible para el análisis (por ejemplo, en línea, archivado o recuperable para la realización de copias de seguridad).**	
TAREAS	

CONTINUA

1.- Mediante entrevistas, examen de los registros de auditoría, examen de la configuración del registro de auditoría, realizar lo siguiente:

*** Verificar que esté registrado todo acceso de personas a datos de titulares de tarjetas**

*** Verificar que estén registradas todas las acciones realizadas por personas con privilegios de raíz o administrativos**

*** Verificar que esté registrado el acceso a todas las pistas de auditoría**

*** Verificar que se registren los intentos de acceso lógico no válidos**

*** Verificar que esté registrado el uso de mecanismos de identificación y autenticación**

2.- Mediante entrevistas y observación, realizar lo siguiente para cada evento auditable:

*** Verificar que la identificación de usuarios se incluya en las entradas del registro**

*** Verificar que el tipo de evento se incluya en las entradas del registro**

*** Verificar que el sello de fecha y hora se incluya en las entradas del registro**

*** Verificar que la indicación de éxito u omisión se incluya en las entradas del registro**

*** Verificar que el origen del evento se incluya en las entradas del registro**

*** Verificar que la identidad o nombre de los datos, componentes del sistema o recursos afectados estén incluidos en las entradas del registro**

*** Verificar que la tecnología de sincronización se implemente y mantenga actualizada**

*** Verificar que sólo los servidores de horario centrales designados reciban señales de tiempo de las fuentes externas y que las señales de tiempo externas estén basadas en la hora internacional**

*** Verificar que los servidores de tiempo central designados interactúen entre sí para mantener un tiempo exacto y que otros servidores internos reciban señales de tiempo sólo de los servidores de tiempo centrales**

*** Revisar las configuraciones del sistema y tanto los valores de configuración como los procesos de sincronización para verificar que cualquier cambio de configuración de tiempo en los sistemas críticos sea registrado, supervisado y revisado**

*** Verificar que los servidores de tiempo acepten actualizaciones de tiempo de fuentes externas específicas, aceptadas por la industria (para evitar que individuos con intenciones fraudulentas cambien el reloj). De forma opcional, se pueden cifrar estas actualizaciones con una clave simétrica, y se pueden crear listas de control de acceso que especifiquen las direcciones IP de equipos cliente a los que se proporcionarán las actualizaciones de tiempo (para evitar el uso no autorizado de servidores de hora internos)**

3.- Entrevistar al administrador del sistema y examinar los permisos para verificar que las pistas de auditoría sean seguras y que no se puedan modificar de la siguiente manera:

*** Verificar que sólo las personas que lo necesiten por motivos relacionados con el trabajo puedan visualizar los archivos de las pistas de auditoría**

*** Verificar que los archivos actuales de las pistas de auditoría estén protegidos contra modificaciones no autorizadas a través de los mecanismos de control de acceso, segregación física y/o segregación de redes**

*** Verificar que se haya realizado copia de seguridad de los archivos actuales de las pistas de auditoría inmediatamente en un servidor de registros central o medios que resulten difíciles**

CONTINUA

de modificar
*** Verificar que registros para tecnologías que interactúan con la parte externa (por ejemplo, inalámbricas, firewalls, DNS, correo) se descarguen o se copien en un servidor de registros central o medios internos**
*** Verificar el uso del software de supervisión de integridad de archivos o de detección de cambios para registros mediante el análisis de los parámetros del sistema, de los archivos supervisados y de los resultados de dicha supervisión**
*** Obtener y examinar las políticas y procedimientos de seguridad para verificar la inclusión de procedimientos de revisión de registros de seguridad al menos una vez al día y que se requiera el seguimiento de las excepciones**
*** Mediante observación y entrevistas, verificar que se realicen revisiones de registros regularmente de todos los componentes del sistema**
*** Obtener y examinar las políticas y los procedimientos de seguridad y verificar que se incluyan las políticas de retención de registros de auditoría y que se requiera la conservación del registro de auditoría durante al menos un año.**
*** Verificar que los registros de auditoría se encuentren disponibles durante al menos un año y que se implementen los procesos para restaurar al menos los registros de los últimos tres meses para el análisis inmediato**

Tabla 10 Proyecto 7 Pruebe con regularidad los sistemas y procesos de seguridad

PROYECTO: Pruebe con regularidad los sistemas y procesos de seguridad	
RESPONSABLE: Por Asignar por parte de la Universidad	
REQUERIMIENTO CUBIERTO	FECHA LIMITE
***Realice análisis internos y externos de vulnerabilidades de red al menos trimestralmente y después de cada cambio significativo en la red (tales como instalaciones de componentes del sistema, cambios en la topología de red, modificaciones en las normas de firewall, actualizaciones de productos).**	
***Realice pruebas de penetración externas e internas al menos una vez al año y después de cualquier actualización o modificación significativa de infraestructuras o aplicaciones (como por ejemplo la actualización del sistema operativo, la adición de una subred al entorno, o la adición de un servidor Web al entorno)**	
-Utilice los sistemas de detección y/o prevención de intrusiones para supervisar el tráfico en el perímetro del entorno de datos de titulares de tarjetas, así como los puntos críticos dentro del entorno de datos de titulares de tarjetas y alerte al personal ante la sospecha de riesgos. Mantenga actualizados todos los motores, líneas base y firmas de detección y prevención de intrusiones.	
-Implemente el software de supervisión de integridad de archivos para alertar al personal ante modificaciones no autorizadas de archivos críticos del sistema, archivos de	

CONTINUA

configuración o archivos de contenido; asimismo configure el software para realizar comparaciones de archivos críticos al menos semanalmente

TAREAS

1.- Verificar que se realicen análisis de vulnerabilidad externa e interna de la manera siguiente:

*** Revisar los informes de los análisis y verificar que se hayan realizado cuatro análisis internos trimestrales durante el período de 12 meses más reciente**

*** Revisar los informes de los análisis y verificar que el proceso de análisis incluya la repetición de los análisis hasta que se obtengan resultados de aprobación o hasta que se resuelvan todas las vulnerabilidades**

*** Verificar que la prueba se haya realizado con un recurso interno calificado o bien que la haya realizado un tercero capacitado, y cuando corresponda, que la persona que realice la prueba sea independiente de la institución**

*** Revisar los resultados de los cuatro trimestres más recientes de análisis de vulnerabilidad externa y verificar que se hayan realizado los cuatro análisis correspondientes al período de 12 meses más reciente**

*** Revisar los resultados de cada análisis trimestral para asegurar que cumplan con los requisitos de la Guía del programa ASV (por ejemplo, no hay vulnerabilidades con calificación mayor que 4.0, según la CVSS y no hay fallas automáticas)**

*** Revisar los informes de los análisis para verificar que hayan sido realizados por un Approved Scanning Vendor (ASV), certificado por las PCI SSC**

*** Inspeccionar la documentación del control de cambios y los informes de análisis para verificar que los componentes del sistemas que hayan sufrido cambios significativos hayan sido analizados**

*** Revisar los informes de los análisis y verificar que el proceso de análisis incluye la repetición de los análisis hasta que:**

*** Para análisis externos, no se hayan registrado vulnerabilidades con puntuaciones mayores que 4.0, según la CVSS.**

*** Para análisis internos, se haya obtenido un resultado de aprobación o todas las vulnerabilidades —Alta‖, como las define el Requisito 6.2 de las PCI DSS, hayan sido resueltas**

*** Obtener y examinar los resultados de la última prueba de penetración para verificar que dichas pruebas se realicen al menos anualmente y después de cualquier cambio significativo realizado en el entorno**

*** Verificar que las vulnerabilidades detectadas se hayan corregido y que se repitan las pruebas**

CONTINUA

*** Verificar que la prueba se haya realizado con un recurso interno calificado o bien que la haya realizado un tercero capacitado, y cuando corresponda, que la persona que realice la prueba sea independiente de la empresa**
*** Verificar que la prueba de penetración incluya pruebas de penetración de la capa de red. Dichas pruebas deben incluir a los componentes que admiten las funciones de red, así como también a los sistemas operativos**
*** Verificar que la prueba de penetración incluya pruebas de penetración de la capa de aplicación. Las pruebas deben incluir, por lo menos, las vulnerabilidades**
*** Verificar el uso de los sistemas de detección y/o prevención de intrusiones y que todo el tráfico en el perímetro del entorno de datos de titulares de tarjetas, así como los puntos críticos dentro del entorno de datos de titulares esté supervisado**
*** Confirmar que estén configurados el IDS y/o IPS para alertar al personal ante la sospecha de riesgos**
*** Examinar la configuración de IDS/IPS y confirme que los dispositivos de IDS/IPS estén configurados, se mantengan y se actualicen según las instrucciones del proveedor para garantizar una protección óptima**
*** Verificar el uso de los productos para supervisión de integridad de archivos en el entorno de datos de titulares de tarjetas mediante la observación de la configuración del sistema y los archivos supervisados, así como también de la revisión de los resultados de las actividades de supervisión**

Tabla 11 Proyecto 8 Mantenga una política que aborde la seguridad de la información para todo el personal

PROYECTO: Mantenga una política que aborde la seguridad de la información para todo el personal	
RESPONSABLE: Por Asignar por parte de la Universidad	
REQUERIMIENTO CUBIERTO	FECHA LIMITE
1.- Desarrollar políticas de utilización para tecnologías críticas para empleados (por ejemplo, tecnologías de acceso remoto, tecnologías inalámbricas, dispositivos electrónicos extraíbles, computadoras portátiles, asistentes digitales/para datos personales [PDA], utilización del correo electrónico y de Internet) para definir el uso adecuado de dichas tecnologías	
TAREAS	
*** Verificar que las políticas de uso requieran ubicaciones aceptables de la tecnología en la red.**	

Dentro del plan de acción expuesto no se consideró persona responsable ni fecha limite ya que las mismas quedan a consideración por parte de la universidad a ser ejecutadas.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

1. De acuerdo al análisis realizado a los medios de comunicación (Lan) se identifica que no existe un proceso establecido formal ni documentado para el manejo de la transaccionalidad de los procesos contables.
2. Al realizar la segmentación de la red se analizó e identificó los diferentes componentes de la red (servidores, switchs, máquinas conectadas a la red, entre otras) de acuerdo como manifiesta la Norma PCI-DSS, para reducir el alcance y costo del análisis forense al aislar los componentes que almacenan, transmiten o procesan información de los tarjetahabientes como aconseja el estandar PCI-DSS.
3. De acuerdo al análisis y evaluación de la red de la Universidad, se determinó que no cuenta con técnicas ni herramientas de análisis forense de detección y prevención por lo que se aconseja la utilización de las herramientas expuestas en el presente proyecto para garantizar que los controles de seguridad continúen reflejando un entorno dinámico de acuerdo como expone el requisito 11 de la norma PCI-DSS.
4. De acuerdo a la metodología utilizada para el análisis forense realizado a la Universidad Tecnológica Equinoccial se identificó que no contempla un nivel adecuado de encriptación o cifrado que asegure la integridad de los datos de los usuarios por lo que se sugiere la implementación de la Norma PCI-DSS la cual con la aplicación de los diferentes requisitos a los que se alinea la institución pretende asegurar los componentes del sistema (servidores, redes, aplicaciones) que admiten entornos de los datos de los titulares de tarjeta.
5. Se identificó que la Universidad no cuenta con mecanismos que permitan rastrear y analizar comportamientos anómalos dentro de la red, y no se

realizan pruebas con regularidad de los componentes de la red y procesos de seguridad de acuerdo como se menciona en los requisitos 10 y 11 de la norma. PCI-DSS.

6. Se propuso un plan de acción para implementar políticas se seguridad de acuerdo a normas internacionales establecidas como es el estándar PCI-DSS que la Universidad tiene la facultad de implementarlo pero que se aconseja aplicarlo a corto plazo ya que de acuerdo al mandato 007-DN-DINARDAP-2013 indica que toda institución debe implementar políticas de seguridad de la información.
7. Luego de realizado el análisis de la norma PCI-DSS se identificó que la Universidad Tecnológica Equinoccial cumple ciertos requisitos de acuerdo a sus políticas de seguridad interna por lo que únicamente es necesario alinearlos al estándar.

6.2. Recomendaciones

1. Establecer políticas de seguridad informática de acuerdo a la norma PCI-DSS dentro de la Universidad, las mismas que deben apuntar a prever casos de intrusiones a los sistemas de información a través de la seguridad, monitoreo y auditorias informáticas permanentes.
2. Implementar controles de seguridad de acuerdo al estándar de PCI-DSS para evitar fraudes a nivel de procesos informáticos.
3. Se recomienda que el software que maneja la Universidad y en especial el sistema SICAF maneje cifrado o encript (Anton A. & Branden R., 2012)ación de datos.
4. Se recomienda a la Universidad la recolección de los diferentes logs generados por las aplicaciones, registro de usuarios, de transacciones entre otras que se encuentran en servidores en puntos diferentes en un solo servidor centralizado tal como indica la norma PCI-DSS y con esto facilitar para la determinación de la causa de un incidente.

5. Se recomienda a la Universidad la implementación del plan expuesto con la finalidad de salvaguardar la información y prevenir fraudes informáticos. La cual servirá a la institución para auditar, mediante la práctica de diversas pruebas técnicas, a los mecanismos de protección instalados y a las condiciones de seguridad aplicadas a los sistemas de información. Asimismo, permitirá detectar las vulnerabilidades de seguridad con el fin de corregirlas.

BIBLIOGRAFÍA

Anonimo. (s.f.). *Metodología para la Implementación de Informática Forense en Sistemas Operativos Windows y Linux*.

Anton A. , C., & Branden R., W. (2012). *Understand and Implement Effective PCI Data Security Standard Compliance.* ELSEVIER.

Areitio, J. (2008). *Seguridad de la Información: Redes, Informática y Sistemas de Información.* España: Paraninfo.

Blog Profesional. (03 de Junio de 2013). *Indicios Digitales*. Obtenido de Análisis forense de la red. Una necesidad presente: http://indiciosdigitales.com/?p=1296

Branden, W., & Chuvakin, A. (2012). *PCI Compliance.* Elsevier - EEUU.

Branden, W., & Chuvakin, A. (2012). *PCI Compliance Understand and Implement Effective PCI Data Security Standard Compliance.* USA: Elsevier.

Council, P. S. (2008). *Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) Exploración de PCI DSS.*

Gomez, D. R. (n/a de n/a de n/a). *cryptomex.org*. Obtenido de Computo Forense Redes: http://cryptomex.org/SlidesForensia/ForensiaRedes.pdf

Jara, H., & Pacheco, F. (2012). *Ethical Hacking: Implementación de un sistema para la gestión de seguridad.* Argentina: RedUsers.

Noguera, B. (29 de Septiembre de 2011). *culturacion.com*. Obtenido de www.culturacion.com/2011/09/para-que-se-usa-un-sniffer

Pacheco Gutierez, A. J. (Octubre de 2009). *Recomendaciones para Análisis Forense en Red*. Obtenido de http://itzamna.bnct.ipn.mx/dspace/bitstream/1233456789/8808/1/165.pdf

PCI QSA y ASV. (Abril de 2009). *https://www.pcisecuritystandars.org/qsa_asv/index.shtml*.

PCI Security Standard Council. (2010). *Norma de Seguridad de Datos de la Industria de Tarjeta de Pago PCI - Cuestionarios de Autoevaluación y Declaración de Cumplimientos.*

PCI Security Standard Council. (2012). *Comprensión de los Objetivos de los Requisitos.*

PCI, P. C. (2012). *PCI Forensic Investigator (PFI).*

Requisitos de las PCI DSS y procedimientos para la evaluación de la seguridad, versión 2.0. (2010).

Untiveros, S. (2012). *AprendaRedes.com*. Obtenido de www.aprendaredes.com/dev/articulos/aprende-a-mirar-dentro-de-la-red-con-un-sniffer.htm

UTA. (s.f.). *http://repo.uta.edu.ec/handle/123456789/2895*. Obtenido de Universidad Técnica de Ambato: http://repo.uta.edu.ec/handle/123456789/2895

Wrigth, S. (2011). *Pci Dss: A practical guide to implementing and maintaining compliance.* Reino Unido: IT Governance.

ANEXOS