UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

PLAN DE PREPARACIÓN FORENSE DIGITAL PARA MAXIMIZAR LA CAPACIDAD DE RECABAR EVIDENCIA DIGITAL EN PROCESOS DE MEDIOS DE PAGO SA, 2016

TESIS PARA OPTAR EL TÍTULO DE
INGENIERO EN COMPUTACIÓN E INFORMÁTICA

FERNANDO FELIPE CRUZALEGUI CRUZALEGUI

Chiclayo, 03 de noviembre del 2016

"PLAN DE PREPARACIÓN FORENSE DIGITAL PARA MAXIMIZAR LA CAPACIDAD DE RECABAR EVIDENCIA DIGITAL EN PROCESOS DE MEDIOS DE PAGO, 2016"

POR:

FERNANDO FELIPE CRUZALEGUI CRUZALEGUI

Presentada a la Facultad de Ciencias Físicas y Matemáticas de la Universidad Nacional Pedro Ruiz Gallo para optar el título de INGENIERO EN COMPUTACIÓN E INFORMÁTICA

APROBADA POR EL JURADO INTEGRADO POR:

MSc. Ing. Jessie Leila Bravo Jaico
PRESIDENTE

Ing. Janet Aquino Lalupú
SECRETARIO

Ing. Consuelo Del Castillo Castro
VOCAL

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE INGENIERIA EN COMPUTACION
E INFORMATICA

PLAN DE PREPARACIÓN FORENSE DIGITAL PARA MAXIMIZAR LA CAPACIDAD DE RECABAR EVIDENCIA DIGITAL EN PROCESOS DE MEDIOS DE PAGO SA, 2016

Ing. Martin Leiva Castillo
Asesor

Bach- Fernando Felipe Cruzalegui Cruzalegui
Autor

Chiclayo, 03 de noviembre del 2016

DEDICATORIA

Para Felipe Cruzalegui Arias.

EPÍGRAFE

El arte de la guerra nos enseña no a confiar en la probabilidad de que el enemigo no se acerque, sino, en nuestra propia preparación para recibirlo; no en la casualidad de que no nos ataque, sino más bien, en que hemos hecho de nuestra posición, un lugar inexpugnable.

Sun Tzu, El Arte de la Guerra

AGRADECIMIENTOS

A mi madre, por todos estos años de sacrificio y por su amor trascendental.

A mi hermano Andrés, por su valiosa, constante e indispensable ayuda.

A mi asesor de tesis, Ing. Martin Leiva Castillo.

A mi tío Juan y a su corazón gigante.

Índice

RESUMEN

El presente trabajo de investigación, realizado entre los meses de abril y agosto del 2016, da cuenta de los hallazgos hechos a partir de la elaboración e implementación de un *Plan de Preparación Forense Digital*, siguiendo los pasos propuestos por el Dr. Robert Rowlingson, para una empresa procesadora de transacciones, en Lima, Perú. Su importancia radica en la necesidad que tiene toda organización de estar preparada para llevar a cabo una investigación forense digital, con un mínimo de interrupción del negocio y la de maximizar su capacidad de recabar evidencia digital, de manera proactiva, alineada con la ciencia forense. Para ello, el experimentador formuló la hipótesis que establecía la posibilidad de maximizar la capacidad de recabar evidencia digital en la Empresa, mediante la elaboración e implementación de un Plan de Preparación Forense Digital. El experimentador revisó y modificó los actuales controles de la Empresa, para crear un marco de gobierno que tome en cuenta la importancia de la evidencia digital. Además de medir la capacidad de recabar evidencia digital de la empresa, se logró identificar la capacidad negativa de recabar evidencia digital, aquella que afecta el almacenamiento de la herramienta de recolección centralizada de logs y las labores asociadas de mantenimiento. Una de las conclusiones de este trabajo, es que, la capacidad de recabar evidencia digital alcanza el 100% solo cuando el número de fuentes de evidencia digital identificadas es igual al número de fuentes de evidencia digital identificadas y recabadas.

PALABRAS CLAVE: Plan, preparación, forense digital.

ABSTRACT

This research, conducted between April and August 2016, shed light on the findings made from the development and implementation of a Forensic Readiness Plan, following the steps proposed by Dr. Robert Rowlingson, for a transaction processing company, in Lima, Peru. Its importance lies on the need for any organization to be prepared to carry out a digital forensic investigation, with minimal business disruption and to maximize its ability to proactively collect digital evidence, aligned with forensic science. In order to do this, the experimenter hypothesized the possibility to maximize the ability to collect digital evidence in the Company, through the development and implementation of a Forensic Readiness Plan. The experimenter reviewed and modified the current controls established in the Company, to create a governance framework that takes into account the importance of digital evidence. In addition to measuring the ability to collect digital evidence in the company, a negative capability of collecting digital evidence was identified; one that affects the storage of a centralized log collection tool and its associated maintenance. One of the conclusions of this work is that the ability to collect digital evidence reaches 100% only when the number of identified sources of digital evidence is equal to the number of identified and collected sources of digital evidence.

KEYWORDS: *Digital forensics, readiness, planning*

I. INTRODUCCIÓN

1.1 Planteamiento del problema

En la actualidad, el delito informático es uno de los problemas más importantes que enfrentan las empresas. Diversos tipos de ataques informáticos son comunes en países, sin importar su grado de desarrollo. El objetivo parece ser uno solo: el dinero. Sin embargo, hay otras causas que mueven a los atacantes. Motivos como la venganza, el deseo de reconocimiento e incluso la sola curiosidad son en algunos casos el móvil del delito informático, estrechamente relacionado a la vulnerabilidad de los sistemas de información. Brett Kelsey, actual vicepresidente y director de "Tecnología para Latino América", afirmó en una entrevista para la agencia EFE de España que este tipo de crímenes "no va a parar de crecer mientras los criminales obtengan ganancias financieras". De acuerdo con el informe "Ciberseguridad 2016" del Banco Interamericano de Desarrollo (BID), solo Brasil, Colombia, Jamaica, Panamá, Trinidad y Tobago y Uruguay tomaron medidas antes las amenazas informáticas, mientras que países como Argentina, Antigua y Barbuda, Bahamas, Costa Rica, Dominicana, El Salvador, Haití, México, Paraguay, Perú y Surinam, se encuentran en el proceso de ensamblar una estrategia de ciberseguridad.

En el Perú contamos con una ley que castiga las actividades delictivas en el ciberespacio, la Ley N° 30096 "Ley de delitos informáticos", promulgada el 21 de octubre del 2013 y una ley que la modifica parcialmente, la Ley N° 30171 "Ley que modifica la Ley 30096, Ley de delitos informáticos", promulgada el 9 y publicada el 10 de marzo del 2014. De esto modo contamos con el marco legal que busca protegernos de acciones contra la información o data, contra los sistemas

informáticos, la indemnidad y libertad sexuales, contra la intimidad y el secreto de las comunicaciones, el patrimonio y la fe pública, en un entorno hecho posible por las tecnologías de la información y las comunicaciones. A pesar de este marco legal, es necesario asegurarse de que tenemos la capacidad de demostrar la comisión de un delito en nuestra empresa. Es preciso tener evidencia admisible ante un juzgado.

La empresa en donde se realizó el presente trabajo de investigación, cuyo giro principal de negocio es el procesamiento de transacciones, pertenece a la industria de las tarjetas de pago, por lo que está en la necesidad de cumplir con normas nacionales e internacionales, de manera que demuestre tomar las medidas exigidas que garantizan la protección de la información procesada, almacenada y transmitida. Esto genera confianza tanto a clientes como al directorio, gerentes, accionistas y colaboradores.

La empresa, a la fecha, no tiene definido un plan de acción, que dé soporte relevante a la investigación de eventos que atenten contra sus políticas de seguridad de información, o contra las leyes peruanas, basado en la evidencia digital que generan, tanto personas, como procesos, por interacción con los recursos de tecnología de información.

Como la mayoría de empresas en el Perú, no existe mayor conciencia al respecto. Grobler y Louwrens (2007) señalan: Las organizaciones desarrollan sus propias arquitecturas de seguridad basadas en las mejores prácticas actuales, por ejemplo ISO 17799 y COBIT. Estas mejores prácticas no consideran la importancia de incorporar controles o procedimientos que aseguren una investigación exitosa. Existe

una necesidad definitiva de adaptar las actuales mejores prácticas en seguridad de información para que incluyan, por ejemplo, ciertos aspectos de la Preparación Forense Digital.

1.2 Objetivos

1.2.1 Objetivo general

Elaborar e implementar un Plan de Preparación Forense Digital para maximizar la capacidad de recabar evidencia digital en una empresa procesadora de transacciones.

1.2.2 Objetivos específicos

a) Recolectar la evidencia digital en los equipos críticos de la empresa.

b) Preservar la evidencia digital, protegiendo su integridad.

c) Presentar la evidencia digital en reportes utilizando la herramienta usada por la Empresa.

d) Comparar la nueva capacidad de recabar evidencia digital con la anterior, en la Empresa

1.3 Importancia

El desarrollo de este proyecto es importante para la empresa porque la dotará de ventajas como lo son tener la capacidad de recolectar evidencia digital sin intervenir con los procesos del negocio, que la evidencia recolectada apunte a posibles ataques a los recursos de la empresa, que el costo de la investigación sea proporcional al

incidente y que la evidencia recolectada tenga una repercusión positiva para la Empresa.

1.4 Justificación

El desarrollo del presente proyecto se justifica porque busca recolectar, preservar y presentar la evidencia digital, para que de este modo, la empresa disponga en todo momento de la información relacionada a todo evento ocurrido en los equipos dentro del alcance del Plan de Preparación Forense Digital y esté preparada ante la necesidad de responder a un incidente de seguridad con evidencia digital, con un uso mínimo necesario, que de otra forma, sería indeterminado.

1.5 Hipótesis

Si se elabora e implementa un Plan de Preparación Forense Digital en la Empresa, entonces incrementará su capacidad de recabar evidencia digital.

II. MARCO TEÓRICO

2.1 Antecedentes

2.1.1 Internacionales

(De Wit, 2013) Planteó como objetivo dotar a una organización de las herramientas para recabar información requerida disponible para realizar un análisis preliminar y posterior adecuado, seguido a un incidente de TI, e incorporar los controles de preparación forense en un marco de trabajo de gobierno en la organización. Concluyó que la preparación forense digital es un estado que permite estar listos para el análisis forense digital. A pesar de los motivos de cumplimiento y de negocio para que las organizaciones busquen una

preparación forense, las publicaciones académicas sobre este tema son escazas y la bibliografía disponible a menudo no describe cómo alcanzar este estado, sino que se concentran en un sub conjunto de asuntos relevantes.

(García Velásquez, 2014) propuso como objetivo desarrollar una metodología de investigación que sirva como referencia y apoyo en las investigaciones dedicadas a identificar al infractor de los delitos informáticos establecidos en el Código Penal Federal, concluyéndose que se consiguió desarrollar una metodología de fácil acceso para la investigación de incidentes de seguridad informática, los mismos que pueden ser considerados cómo delitos informáticos. La metodología desarrollada ofrece una guía clara y precisa para realizar una investigación basada en Computación Forense, a pesar de que cada investigación es diferente, la forma estructurada de la metodología provee bases sólidas para llevar a cabo cualquier investigación.

2.1.2 Nacionales

(Morales Zamudio, 2010) estableció como objetivo de tesis, mostrar el diseño de una solución de la implantación de un Sistema de Seguridad Informática en empresas estatales y se concluyó que la aprobación de los documentos es un factor crítico de éxito de un proyecto, que por medio de la ejecución constante de simulaciones de ataques y por el fortalecimiento de las tecnologías por parte de los administradores de red, se espera que el establecimiento de los equipos disminuya el nivel de riesgo de las tecnologías de información, que el trabajo en conjunto permite mitigar los riesgos y no

concentrarse en quién tiene la culpa cuando suceda un incidente de seguridad informática.

(Palomino Pio, 2008) Propuso mejorar el nivel de seguridad de los accesos a los 32 servidores que contienen información crítica de la empresa, cumpliendo por lo menos con el 90% de buenas prácticas, establecido como estándar de control de accesos en los servidores de la empresa, concluyéndose que 28 de 32 plataformas de sistemas de la Empresa (87.5%) superan el cumplimiento del 90% de recomendaciones de buenas prácticas de control de accesos para tener un nivel adecuado de Seguridad de Información. Se mejoraron los niveles de seguridad de información. En promedio para todas las plataformas se tiene un nivel de seguridad de 91.6% a setiembre del 2006, mejorando en un 62.3% comparado con la medición realizada en marzo del 2006.

2.1.3 Regionales

(Vallejos Saravia & Suyon Urquizo, 2010) fijaron como objetivo desarrollar un Plan de Riesgo para la Sub-Gerencia de Racionalización e Informática de la Sede del Gobierno Regional Lambayeque, utilizando metodología “MAGERIT” con el fin de obtener un documento normativo que ayude a tener noción de las posibles amenazas que puedan atentar contra los activos y obtener un Plan de Contingencia, concluyendo que se logró desarrollar un Plan de Riesgo, logrando así obtener un documento normativo que ayude a tener noción de las posibles amenazas que puedan atentar contra los activos y poder así tener el Plan de Contingencia y de Recuperación para que la institución

pueda seguir laborando con normalidad a pesar de los posibles desastres que puedan ocurrir.

(Seytuque Limo, 2008) planteó desarrollar un modelo de políticas de seguridad y gestión de tecnología de la información y comunicación, aplicado al Gobierno Regional de Lambayeque, concluyendo que la aplicación de un Sistema de Tecnologías de la Información y Comunicación, constituye un medio para un fin, no un fin en sí mismo; no se trata solamente de manuales, políticas, normas y directivas, sino de personas que participen en cada proceso de información que se gestiona a través de las distintas unidades orgánicas y oficinas administrativas de la Sede del Gobierno Regional.

2.2 Base teórica

2.2.1. Seguridad de la Información

Según lo indica la Superintendencia de Banca, Seguros y AFP (2009) la seguridad de la información es la característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos de que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad, definidos de la siguiente manera:

a) Confidencialidad: La información debe ser accesible solo a aquellos que se encuentren debidamente autorizados.

b) Integridad: La información debe ser completa, exacta y válida.

c) Disponibilidad: La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

Estos tres elementos constituyen la triada de la seguridad de la información. Nos protegemos contra la pérdida de confidencialidad al asegurarnos que ningún usuario no autorizado pueda acceder a información. Este proceso se inicia al identificar y autorizar al usuario y luego implementar un sistema de control de accesos para restringir el mismo. La encriptación provee otra capa de protección para la confidencialidad, la misma que solo es posible garantizar cuando se implementan algoritmos de encriptación seguros y se implementan medidas de seguridad estándar.

Los controles de integridad previenen cualquier modificación no deseada o no autorizada de data o de sistemas. La utilización de un número de hash o los registros o logs de auditoría, son dos maneras de proteger la integridad de la información. El hash detectará la alteración de data y alertará al personal correspondiente de la pérdida de integridad del recurso. Por otro lado, los logs de auditoría mostrarán la actividad llevada a cabo sobre un recurso, como qué se modificó, quién lo modificó y cuándo ocurrió.

Prevenir la pérdida de disponibilidad de la información asegura que los sistemas informáticos y la data estén disponibles cuando se les necesite. Algunas tecnologías empleadas por las organizaciones para garantizar la disponibilidad de la información, son: Backups, discos redundantes, servidores redundantes, conexiones redundantes, sitios (oficinas) redundantes.

Adicionalmente al uso de tecnologías tolerantes a fallas y redundantes, las organizaciones crean planes de continuidad de negocio y planes de recuperación de desastres lo que ayuda a mantener la disponibilidad de los sistemas críticos, incluso después de un desastre.

La Seguridad de la Información se vale de la Seguridad Informática para proteger el entorno de la información procesada por medios informáticos. Veamos a continuación su definición.

2.2.1.1 Seguridad Informática

De acuerdo a la revista PC Magazine (2016) la seguridad informática es la protección de data, redes, y del poder informático. La protección de la data es lo más importante. La protección de las redes es importante para prevenir la pérdida de los recursos de servidores así como también para impedir que la red tenga un uso ilegal.

2.2.2. Ciencias Forenses

De acuerdo con el International Council of E-Commerce Consultants (2012) las ciencias forenses son definidas como la aplicación de las ciencias físicas a la ley, en la búsqueda de la verdad en asuntos civiles, criminales y del comportamiento social, con el fin de que la injusticia no sea cometida contra ningún miembro de la sociedad.

El propósito principal de cualquier investigación forense es el de determinar el valor de la evidencia en la escena del crimen y la evidencia

asociada retenida. Las funciones de los científicos forenses incluyen el análisis apropiado de la evidencia física, brindar un testimonio experto ante una corte y la de brindar capacitación en cuanto a reconocimiento, recolección y preservación de evidencia física se refiere.

De esta ciencia se deriva la llamada "Computer Forensics" de traducción aceptada como Computación Forense o Informática Forense, y cuya definición ha sido incluida en la presente base teórica. Existe un concepto que engloba la Computación Forense, el mismo que veremos a continuación.

2.2.2.1 Forense Digital

Cano Martinez (2009) traduce el vocablo inglés Digital Forensics como "Forensia Digital", sin embargo, el autor de este proyecto ha creído conveniente el uso del témino "Forense Digital" puesto que no ha encontrado la palabra "forensia" en ningún diccionario.

Sachowsky (2016) define el concepto de Forense Digital como una disciplina que se adhiere a la disciplina de las ciencias forenses y como la aplicación de la ciencia al Derecho, en donde se utilizan principios científicos, metodologías y técnicas durante una investigación.

La disciplina forense digital tiene por alcance todo medio informático, todo dispositivo digital que almacene información, sea esta volátil o no volátil.

2.2.2.2 Computación Forense

De acuerdo al mexicano Cano Martinez (2009), es la disciplina de las ciencias forenses que, considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso.

Para Gibson (2009), la Computación Forense es la ciencia de examinar e inspeccionar un sistema informático para hallar evidencia de un evento o de un crimen. La examinación incluye la recuperación de data almacenada o transmitida por cualquier dispositivo electrónico. Un objetivo primario cuando se identifica y recupera evidencia digital es el de preservar su integridad. De esta forma, los expertos forenses pueden analizarla e incluso utilizarla en un proceso legal, de ser necesario. Los investigadores son cuidadosos para asegurar que no modifiquen la evidencia mientras la recolectan, luego de la cual la protegen. Los Informáticos Forenses expertos tienen estos mismos objetivos para poder indagar sobre la comisión de un delito informático. La única diferencia es que los Informáticos Forenses utilizan herramientas y técnicas diferentes cuando investigan un incidente.

2.2.2.3 Evolución de la Computación Forense

La evolución de la computación forense es como se indica a continuación, según lo detalla el International Council of E-Commerce Counsultants (2012):

- **1822 – 1911**

  Francis Galton realizó el primer estudio registrado de huellas digitales para capturar criminales acusados de asesinato.

- **1887 – 1954**

  Leone Lattes fue la primera persona en usar grupos sanguíneos para poder relacionar criminales con un crimen determinado.

- **1891 – 1955**

  Calvin Goddard se convirtió en la primera persona en hacer uso de comparaciones de armas de fuego y de balas para resolver muchos casos judiciales no resueltos.

- **1858 – 1946**

  Albert Osborn fue la primera persona en desarrollar las características esenciales de la documentación de evidencia durante el proceso de examinación.

- **1847 – 1915**

  Hans Gross fue la primera persona en usar un estudio científico para liderar una investigación criminalística.

- **1932**

  El FBI creó un laboratorio para brindar servicios forenses a todos los agentes de campo y otras autoridades judiciales.

- **1984**

  Se desarrolló el Equipo Informático de Análisis y Respuesta (CART, por sus siglas en inglés) para brindar apoyo a las oficinas de campo del FBI en búsqueda de evidencia digital.

- **1993**

  Se celebró la Primera Conferencia Internacional sobre evidencia informática, en los Estados Unidos de América.

- **1995**

  Se formó la "International Organization on Computer Evidence" (IOCE) para brindar un fórum a todas las agencias policiales a nivel mundial para intercambiar información sobre investigaciones de delitos informáticos y otros asuntos relacionados con la computación forense.

- **1998**

  Se formó el “International Forensic Science Symposium” para brindar un fórum para los administradores forenses y para intercambiar información.

- **2000**

  Se estableció el primer “Regional Computer Forensic Laboratory” del FBI, para la examinación de la evidencia digital, como soporte a las investigaciones criminales tales como robo de identidad, hackeo, virus informáticos, terrorismo, fraude de inversión, cyber acoso, tráfico de drogas, phishing, spoofing, programación errónea, fraude de tarjetas de crédito, fraude de subastas en línea, spam, entre otros.

- **2006**

  Es establece en México D.F. “Mattica” el primer laboratorio privado de investigaciones digitales en América Latina.

2.2.2.4 Objetivos de la Computación Forense

De acuerdo al International Council of E-Commerce Consultants (2012), las herramientas y metodologías de la Computación Forense, son componentes principales del estado de preparación para la recuperación de desastres en una organización, y juega un rol decisivo para subsanar un incidente informático. El objetivo general de todas

las fases de la computación forense, por ejemplo, preservación, identificación, extracción, interpretación y documentación, es detectar el incidente informático, identificar al intruso y procesar al perpetrador en un juzgado. Estos objetivos pueden ser resumidos de la siguiente forma:

- Recuperar, analizar y preservar computadoras y el material asociado, de manera tal que pueda ser presentado como evidencia ante un juzgado.
- Identificar la evidencia en un corto plazo, estimar el impacto potencial de la actividad maliciosa sobre la víctima y evaluar la intención e identidad del perpetrador.

2.2.2.5 Necesidad de la Computación Forense

Un exponencial incremento en el número de delitos informáticos y litigios donde grandes organizaciones estuvieron involucradas, ha resaltado lo necesario que es la Computación Forense, de acuerdo con el International Council of E-Commerce Consultants (2012). Se ha convertido en una necesidad para las organizaciones, contratar el servicio de una agencia de Computación Forense, o un experto en Computación Forense y tecnologías relacionadas. Las pérdidas financieras ocasionadas debido a los delitos informáticos, también han contribuido al renovado interés en la Computación Forense, la misma que tiene un papel importante en el seguimiento de las pistas del ciber-criminal. El rol principal de la computación forense es:

- Asegurar la integridad de la evidencia digital generada por las fuentes de información, así como su continuidad en la infraestructura de la organización.
- Ayudar a la organización a capturar información importante, cuando sus sistemas informáticos o redes, hayan sido comprometidos. Esto conllevará a evidenciar la actividad no permitida o ilegal del atacante identificado.
- Extraer, procesar e interpretar la evidencia digital, de modo que pruebe ante un juzgado, las acciones del atacante, o la inocencia del acusado.
- En el ámbito internacional, la Computación Forense ayuda a seguir el rastro a los miembros de grupos terroristas, de manera eficiente. Ellos usan el internet como un medio de comunicación, por lo que pueden ser rastreados, y sus planes, descubiertos.
- Cuidar el tiempo y el dinero de la organización. Muchos gerentes destinan una gran parte del presupuesto de TI, para la seguridad de las redes y de los ordenadores, por ejemplo, para adquirir herramientas SIEM (*Security Information and Event Management*) en las cuales puedan no solo almacenar los registros de auditoría generados por los dispositivos y aplicaciones, sino también, analizar la

información, generar reportes y alertas a las partes interesadas.

- Hacer seguimiento a casos complicados tales como pornografía infantil, fraude, etc.

2.2.2.6 Preparación Forense Digital

El concepto de Preparación Forense Digital fue acuñado por John Tan (2001). Según el Dr. Robert Rowlingson (2004) visto desde una perspectiva empresarial, la Preparación Forense Digital es la habilidad de una organización para maximizar su potencial para usar evidencia digital cuando esta sea requerida.

2.2.2.7 Beneficios de la Preparación Forense Digital

La preparación forense digital permite a las organizaciones hacer un uso óptimo de la evidencia digital en un período de tiempo y costo de investigación limitados, según señañala el International Council of E-Commerce Constultants (2012). La preparación forense digital también minimiza el riesgo de amenaza interna. Actúa como una medida preventiva. Contar con una preparación forense digital, permite a una organización contar con evidencia digital íntegra, válida ante las fuerzas del orden público.

Algunos de los beneficios de la preparación forense digital, en una organización, son:

- Recabar evidencia digital para actuar en defensa de la organización, de ser sometida a un proceso legal.
- Disuadir al atacante interno, mediante la recolección proactiva de evidencia (eliminar o no recolectar evidencia digitales en las fuentes críticas de la organización, es ayudar a cubrir los rastros de un atacante interno o externo).
- En el caso de un incidente de mayor envergadura, se puede llevar a cabo una investigación rápida y eficiente, así como también, se pueden tomar las acciones necesarias, con una mínima interrupción del negocio (personal, procesos).
- Reducir significativamente los costos y tiempos de una investigación interna, o externa a la organización, usando un enfoque sistemático sobre el almacenamiento de evidencia digital.
- La preparación forense digital puede extender el ámbito de la seguridad de la información a la amenaza que representa el ciber crimen como el robo de propiedad intelectual, fraude, extorsión, etc.
- Demostrar debida diligencia y un buen gobierno corporativo de los recursos de información de la compañía.
- Demostrar que se han cumplido con requerimientos regulatorios, como PCI DSS, SSAE16. SOX, etc.

- Mejorar o facilitar la interacción con las autoridades gubernamentales.
- Mejorar la perspectiva para una acción legal exitosa para la organización.
- Brindar evidencia digital para resolver un litigio comercial.
- Respaldar sanciones a empleados, basándose en la evidencia digital.

2.2.2.8 Objetivos de la Preparación Forense Digital

La evidencia digital es necesaria para respaldar un proceso de investigación forense digital. Una organización, por lo tanto, necesita acceder a la evidencia digital real. El enfoque de la preparación forense digital consiste en aquellas acciones técnicas y no técnicas para maximizar la capacidad de una organización para usar evidencia digital, en su beneficio. De acuerdo con el International Council of E-Commerce Consultants (2012) el objetivo principal de la preparación forense digital es el de ser el soporte de los requisitos de una organización para usar evidencia digital. Los objetivos de la preparación forense digital son:

- Recabar evidencia digital aceptable desde el punto de vista forense digital, sin interferir con los procesos del negocio.

- Recabar evidencia digital apuntando a los potenciales delitos y litigios que podrían impactar de forma negativa a una organización.
- Permitir que una investigación proceda a un costo proporcional al incidente.
- Asegurar que la evidencia digital tenga un impacto positivo en el resultado de una acción legal.

2.2.3. Plan de Preparación Forense Digital

Existe un proceso compuesto por diez pasos para alcanzar la preparación forense digital, propuesto por el Dr. Robert Rowlingson (2004). Estos constituyen el plan de preparación forense digital y son los siguientes:

1. Definir los escenarios de negocio que requieren evidencia digital.
2. Identificar las fuentes disponibles y diferentes tipos de potencial evidencia.
3. Determinar el requisito de colección de la evidencia.
4. Establecer una capacidad para recolectar de forma segura y legal evidencia admisible.
5. Establecer una política para un almacenamiento y tratamiento seguros de la potencial evidencia.
6. Asegurar que cualquier monitoreo apunte a detectar y disuadir incidentes mayores.
7. Especificar las circunstancias en las que deberá iniciarse una investigación formal completa, la misma que podrá usar evidencia digital.
8. Capacitar al personal en concientización de incidentes, de modo que todos aquellos involucrados comprendan sus roles en el proceso de evidencia digital y las sensibilidades legales de la misma.

9. Documentar un caso basado en evidencia describiendo el incidente y su impacto.
10. Asegurar una asesoría legal para facilitar la acción en respuesta al incidente.

III. MATERIAL Y MÉTODOS

3.1 Procedimiento de Investigación

Se revisó la bibliografía disponible sobre el tema "Preparación Forense Digital". Se analizó la situación problemática de la Empresa y cómo ayuda la elaboración e implementación de un "Plan de Preparación Forense Digital" para maximizar la capacidad de recabar evidencia digital, así como también para ordenar y mejorar la visibilidad de los elementos monitoreados, apoyar el cumplimiento del estándar PCI DSS, establecer un nivel de preparación del personal responsable del proceso forense digital, y el tener una asesoría legal ante el quebrantamiento de las leyes peruanas, dentro de la Empresa, haciendo uso de sus recursos tecnológicos.

3.2 Elementos muestrales

Para determinar la muestra de la población, se usó la siguiente fórmula:

$$n = \frac{N * Z_{\alpha}^{2} * p * q}{d_{2} * (N-1) + Z_{\alpha}^{2} * p * q}$$

Donde:

N=Población de fuentes de evidencia digital identificadas
P=Valor de la proporción que se asume 0.05
q=Probabilidad en contra
d= Precisión (con 5%)
Z=Nivel de confianza (1.96 si la seguridad es 95%)

Para este cálculo, se tomaron los siguientes valores:

N=98 p=0.05 d=0.05 Z (95%)=1.96

Luego, el tamaño de la muestra es igual a 4 fuentes de evidencia digital, del entorno de datos del tarjetahabiente (Tabla 1)

Fuentes de evidencia digital identificadas	CANTIDAD
Controlador de Dominio	01
Antivirus	01
Anti-Spam	01
IPS	01

Tabla 1: Componentes seleccionados

3.3 Instrumentos

Los siguientes controles internos de la empresa, fueron utilizados como instrumentos para llevar a cabo la investigación (tabla 2).

Controles Administrativos	Controles Técnicos	Controles Físicos
• Proceso de 10 pasos para la preparación forense digital, propuesto por Dr. Robert Rowlingson (2004). • Estándar de Seguridad de Datos PCI DSS versión 3.2 (2016) • Política de Seguridad de la Información de la Empresa, 2016. • Plan de Respuesta a Incidentes, de la Empresa, 2016.	• Herramienta SIEM usada por la Empresa	• Controles de acceso físico hacia la herramienta SIEM usada por la Empresa. • Controles de acceso físico hacia las fuentes de evidencia digital crítica.

Tabla 2: Instrumentos

IV. RESULTADOS

Para alcanzar los objetivos de esta investigación, fue necesaria la creación de un nuevo control administrativo como lo es el Plan de Preparación Forense Digital, así como la modificación de las Políticas de Seguridad de Información y el Plan de Respuesta a Incidentes de la Empresa. La tabla 3 nos muestra el detalle para cada control dentro del alcance de la investigación.

Controles Administrativos	**Controles Técnicos**	**Controles Físicos**
• Plan de Preparación Forense Digital (Creado). • Política de Seguridad de la Información de la Empresa, 2016 (Modificado). • Plan de Respuesta a Incidentes, de la Empresa, 2016 (Modificado).	• Herramienta SIEM usada por la Empresa (Re-configurada)	• Controles de acceso físico hacia la herramienta SIEM usada por la Empresa (Revisados). • Controles de acceso físico hacia las fuentes de evidencia digital crítica (Revisado).

Tabla 3: Controles desarrollados

Los hallazgos del trabajo de investigación son:

4.1 Equipos críticos

El plan de preparación forense digital permitió identificar los equipos críticos (fuentes de evidencia digital crítica) en la empresa, desde una perspectiva de riesgo del negocio. Basta con realizar una nueva evaluación de riesgo de negocio, como son los escenarios de fraude, fuga de información, etc., para poder validar si existe alguna fuente de evidencia digital que necesite ser agregada al alcance de fuentes de

evidencia digital crítica (*Anexo 8.2, paso 2*). A partir de este paso, podemos iniciar el proceso de envío de registros de auditoría hacia la herramienta SIEM con la que cuenta la Empresa y de esta forma consolidar el proceso de recolectar evidencia digital de manera centralizada.

Tabla 4: Identificación de Fuentes

4.2 Integridad de la Evidencia Digital

El plan de preparación forense digital sirvió de guía para realizar los cambios necesarios a los controles administrativos, técnicos y físicos, para proteger la integridad de la evidencia digital, así como también su disponibilidad y confidencialidad. Como se indica en el paso 3 del Anexo 8.2, se modificó la Política de Seguridad de Información de la Empresa, agregando el inciso 12.5.6.1 Recolección de evidencia digital. En él se diferencian dos escenarios de recolección de evidencia.

El primero obedece al envío en tiempo real y centralizado de los logs de las fuentes de evidencia digital, para un análisis y almacenamiento centralizados. En este punto, el control administrativo garantiza la continuidad de la gestión de la evidencia digital bajo este enfoque que busca alcanzar el segundo objetivo específico de esta investigación.

En el segundo caso, se asume la necesidad de llevar a cabo una recolección de evidencia in situ, para lo cual, se modificó el *Plan de Respuesta a Incidentes* de la Empresa, de manera que sirva de guía cuando ocurra un incidente de seguridad que por sus características, lo demande.

En ambos casos, los controles Administrativos (establecimiento de políticas y definición del plan de preparación forense, así como la modificación del plan de respuesta a incidentes), Físicos (validación de los controles de acceso físico al SIEM y al área de almacenamiento de los activos críticos de la empresa como las cintas de respaldo de información) y Técnicos (configuración del SIEM para asegurar que el control de acceso basado en roles sea implementado para cumplir lo establecido por los controles administrativos), han sido adecuados para garantizar la integridad de la evidencia digital, de modo que pueda participar de una investigación forense digital y establecer los hechos a partir del análisis.

Antes de la elaboración e implementación del Plan de Preparación Forense Digital, la integridad de la evidencia digital era un tema de poca importancia. Tras la implementación, la integridad de la evidencia digital es crítica en la Empresa.

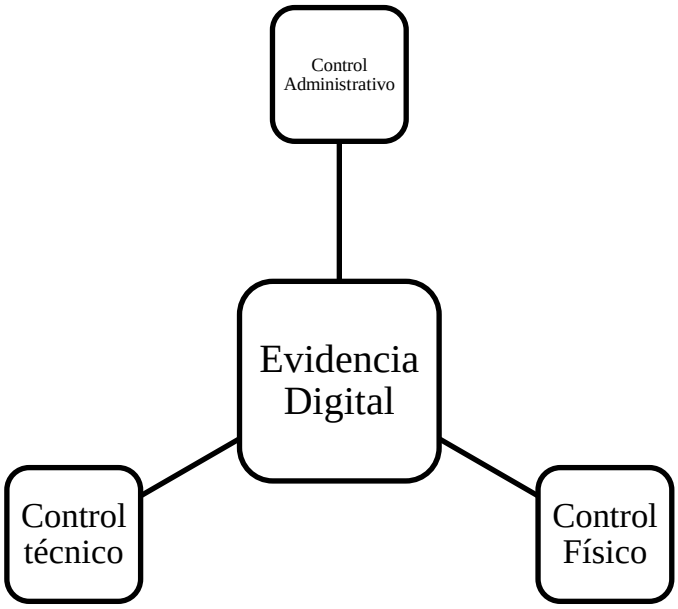

Tabla 5: Cuidado de la evidencia digital

4.3 Reportes

La herramienta SIEM utilizada por la empresa (Ver Anexo 8.4), permitió elaborar reportes a partir de los logs enviados por los equipos críticos, también llamados, por el experimentador, *fuentes de evidencia digital crítica*. Es importante anotar que el uso de esta herramienta, fue trascendental para la ejecución del Plan de Preparación Forense Digital, y sin ella, habría sido necesario realizar un análisis de costo beneficio para la adquisición de una herramienta para recolección de logs, u otra con esta función y funciones adicionales como el análisis y correlación de eventos, como se muestra en la siguiente tabla.

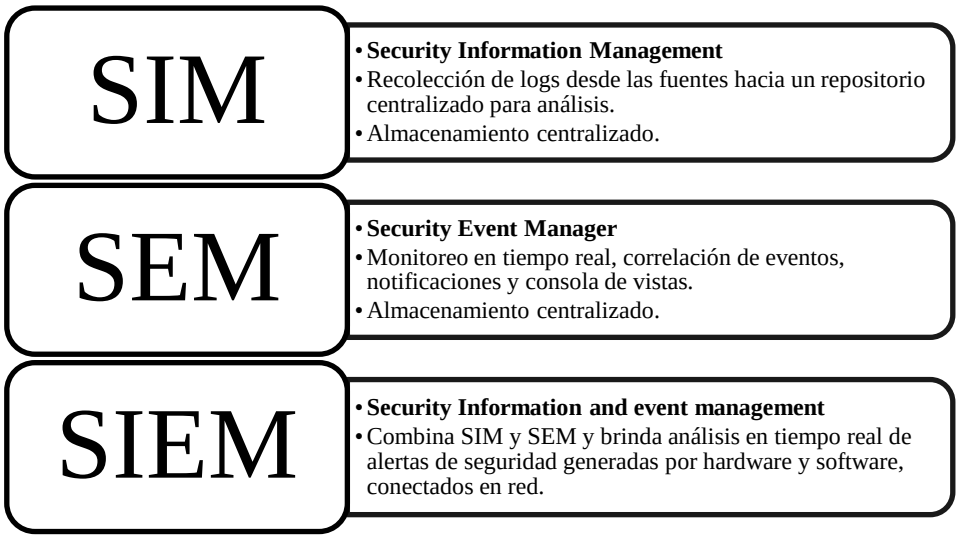

Tabla 6: SIM, SEM y SIEM

La siguiente tabla muestra la cantidad de reportes generados por cada elemento muestral:

ELEMENTO MUESTRAL	N° DE REPORTES
Controlador de Dominio	10
Antivirus	03
Anti-Spam	03
IPS	05
Total	21

Tabla 7: N° Total de Reportes

4.4 Comparativo

Para poder comparar la capacidad de recabar evidencia digital en la empresa antes y después de la implementación del Plan de Preparación Forense Digital, se elaboró la siguiente fórmula:

$$C_r = \frac{F_{ir}}{F_i} * 100\%$$

C_r	Capacidad de recabar evidencia digital (expresada en porcentaje).
F_{ir}	Número de Fuentes de evidencia digital identificada y recabada.
F_i	Número de Fuentes de evidencia digital identificadas

De esta fórmula podemos deducir que el número de fuentes de evidencia digital recabada debe ser igual al número de fuentes de evidencia digital identificadas para que la capacidad de recabar evidencia digital se encuentre en su punto máximo.

La siguiente tabla muestra el valor de la capacidad de recabar evidencia digital, antes y después, de implementar el plan de preparación forense digital en la organización.

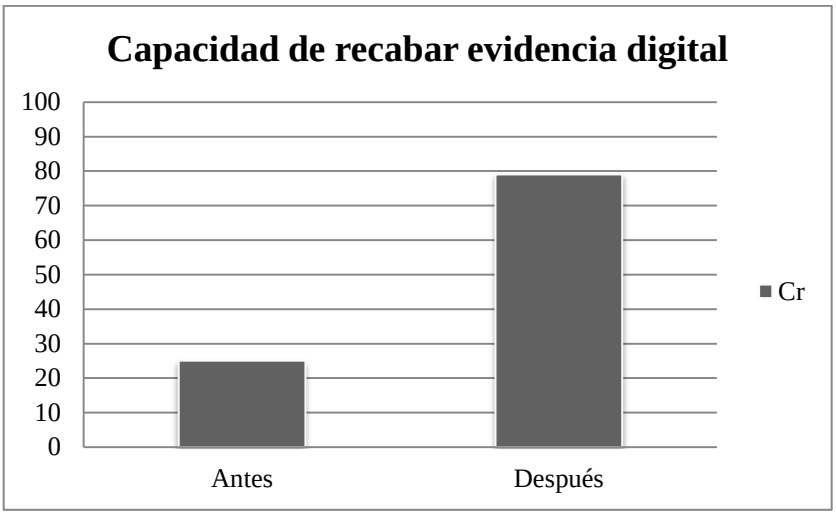

Tabla 8: Capacidad de recabar evidencia digital

Fue importante el hallazgo de un indicador que representa el número de fuentes de evidencia digital no identificadas, recabadas. Es decir, toda aquella fuente de evidencia digital que no ha sido identificada bajo un análisis de riesgo de negocio, sin embargo, la información de actividad registrada en sus logs, es enviada al SIEM, impactando el almacenamiento interno de la herramienta.

El experimentador nombró este indicador como "Capacidad Negativa de Recabar Evidencia Digital" definida por la siguiente fórmula:

$$C_{nr} = \frac{F_{nir}}{F_i} * 100\%$$

C_{nr}	Capacidad negativa de recabar evidencia digital
F_{nir}	Número de Fuentes de evidencia digital **no** identificada, recabada.
F_i	Número de Fuentes de evidencia digital identificadas

El plan de preparación forense permitió reducir la Capacidad Negativa de Recabar Evidencia Digital en la Empresa a cero, valor que es el esperado para esta variable.

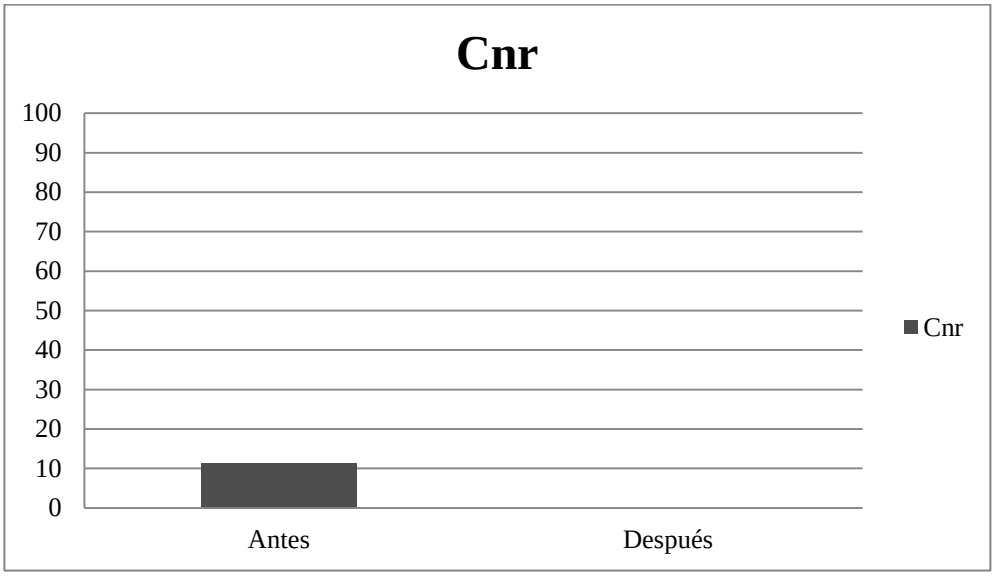

Tabla 9: Capacidad Negativa de Recabar Evidencia Digital

El impacto que genere la capacidad negativa de recabar evidencia digital dependerá de eventos como el mantenimiento del espacio en disco de almacenamiento de la herramienta y de la habilidad de la herramienta para sobre-escribir información nueva sobre información antigua. Para ambos casos, recolectar evidencia no necesaria, según análisis de riesgo de negocio NO es productivo.

El siguiente cuadro muestra un ejemplo del impacto de esta variable, desde diciembre del 2015 a julio del 2016

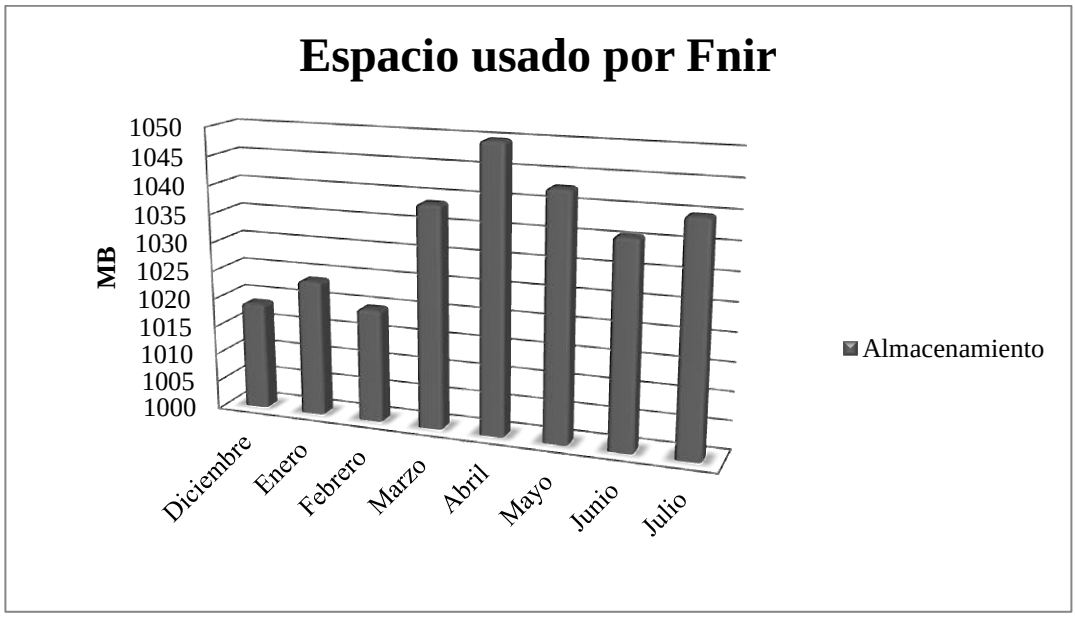

Tabla 10 Fuente no identificada, recabada

Del ejemplo de esta tabla, podemos afirmar que la empresa pudo haber ahorrado un total de 8271 MB es decir 8.07 GB de almacenamiento en la herramienta SIEM de haberse ejecutado un análisis de riesgo de negocio antes de conectar la fuente de evidencia digital con la herramienta SIEM, para envío de logs NO relevantes, es decir, para aquellos que provengan de fuentes de evidencia digital NO identificadas luego del análisis de riesgos para el negocio.

4.5 Cumplimiento

La Empresa debe de cumplir 32 de los 34 sub requisitos que componen el requisito 10 de la norma PCI DSS versión 3.2 "*rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta*". El plan de preparación forense digital tuvo la capacidad para soportar el cumplimiento del 94.12% del total de sub requisitos del requerimiento 10 de PCI DSS versión 3.2. (Anexo 8.3). Con la

implementación del Plan de Preparación Forense Digital, la Empresa pudo cumplir 96.88% del requerimiento 10 de PCI DSS versión 3.2.

V. DISCUSIÓN

La identificación de los equipos críticos, el cuidado de la integridad y disponibilidad de la evidencia digital, el uso de la herramienta SIEM para la generación de reportes, a partir de la información recabada en los logs enviados por las fuentes de evidencia, la posibilidad de medir la capacidad de recabar evidencia digital usando valores cuantitativos y el cumplimiento del requisito 10 de PCI DSS versión 3.2, conformaron los resultados de esta investigación cuyo objetivo fue el elaborar e implementar un plan de preparación forense digital para maximizar la capacidad de recabar evidencia digital en una empresa procesadora de transacciones, encontró en la hipótesis "*Si se elabora e implementa un Plan de Preparación Forense Digital en la Empresa, entonces incrementará su capacidad de recabar evidencia digital*", más de una respuesta al problema planteado inicialmente, el cual fue que, la empresa, no tenía definido un plan de acción, que dé soporte relevante a la investigación de eventos que atenten contra sus políticas de seguridad de información, o contra las leyes peruanas, basado en la evidencia digital que generan, tanto personas, como procesos, por interacción con los recursos de tecnología de información.

La identificación de los equipos críticos fue un proceso obtenido mediante la definición del escenario de riesgo del negocio de la Empresa: "Cumplimiento de PCI DSS". Dado que la empresa debe acreditar ante el foro mundial PCI SSC (Payment Card Industry Security Standards Council), que cumple con los 12 requisitos de la norma PCI

DSS, solicitados por esta entidad, el proceso de acreditación es crítico y su incumplimiento representa un alto riesgo de negocio. La empresa vería afectada su imagen, prestigio, posible pérdida de clientes actuales y prospectos, entre otros. El experimentador tomó el total de equipos que se encuentran en el alcance de PCI DSS en la empresa, es decir, los equipos que procesan, almacenan o transmiten datos del tarjetahabiente o información de autenticación sensible, y llamó a esta cantidad, "número de fuentes identificadas". El experimentador nombró "número de fuentes identificadas y recabadas", al total de equipos identificados que envían logs a la herramienta SIEM de la empresa.

La integridad de la evidencia digital recabada fue asegurada tras la revisión y adecuación de los controles administrativos, técnicos y físicos en la Empresa. Se realizaron cambios en los controles administrativos como son la Política de Seguridad de Información y el Plan de Respuesta a Incidentes, de manera que la integridad y disponibilidad de la evidencia digital, se mantengan desde su nacimiento hasta su eliminación. Tales cambios implican la observación de dos escenarios; en el primero, la evidencia digital se encuentra almacenada en un repositorio, el cual es la herramienta SIEM de la empresa. En él, la evidencia digital goza de protección a nivel de aplicación y es necesario asegurar su almacenamiento mediante controles técnicos, como son, la configuración de la herramienta de modo que se asignen roles solo con los permisos necesarios para que el personal con acceso a la herramienta SIEM pueda realizar su función. De este modo, se evitarán acciones no deseadas como una eliminación casual o con un fin mal intencionado. En el segundo escenario, la evidencia digital se encuentra en la escena del crimen y se modificó el Plan de Respuesta a Incidentes para establecer

que es el Equipo de Primera Respuesta (Personal de servicio en horario de oficina y en horario de 24 horas, los siete días de la semana) aquel que debe acudir a la escena a tomar las primeras medidas necesarias antes de la llegada del personal Forense Digital, delegado a una consultora que brinda este servicio para la Empresa.

La creación de reportes a partir de los logs, considerados por el experimentador fuente primaria de evidencia digital, se llevó a cabo con el uso de la herramienta SIEM usada por la Empresa. Para este paso, se contó con el apoyo del personal de Soporte de la herramienta, cuyo uso requiere de un conocimiento técnico avanzado que permita realizar consultas sobre los eventos registrados en los logs para poder generar los reportes requeridos, usando un lenguaje de consulta. Para crear un reporte a partir de la información de logs recabada por la herramienta SIEM, se debe de analizar qué eventos necesitamos reportes. Cuando tenemos identificados los eventos, debemos asegurarnos de que los mismos, tengan un código asignado por el sistema operativo instalado en la fuente de evidencia digital. El SIEM, en algunos casos, necesitará de la creación de un "parser" o intérprete que le permita mostrar toda la información recibida en el log de la fuente digital. Esto es crítico para presentar la información completa.

Para el caso de las 04 fuentes de evidencia digital identificadas, solo el IPS (Sistema de Prevención de Intrusos) necesitó la creación de un parser. La actividad fue llevada a cabo por el proveedor de la herramienta.

El comparativo realizado entre la capacidad de recabar evidencia digital antes y después de elaborar e implementar el Plan de Preparación Forense Digital en la Empresa, arrojó un valor de 68.35% de incremento. Tras implementar el Plan de

Preparación Forense Digital la capacidad de recabar evidencia digital tocará su punto máximo solo si el número de fuentes de evidencia digital identificada es igual al total de fuentes de evidencia digital identificada y recabada. Además, se identificó el indicador de fuentes de evidencia digital no identificada y recabada, el cual no contribuye a la investigación, sino que impacta de manera negativa el almacenamiento del SIEM o recolector de logs, así como también, el trabajo de respaldo, y mantenimiento de la herramienta.

La Empresa debe de cumplir 32 de los 34 sub requisitos de PCI DSS, de forma anual, para recibir una certificación internacional que la acredite como una empresa segura para el tratamiento de datos de sus clientes, los tarjetahabientes. Mientras que el Plan de Preparación Forense Digital permite cumplir el 94.12% de los sub requisitos del requerimiento 10 de PCI DSS versión 3.2, la implementación de este plan permitió cumplir el 96.88% de los sub requisitos mencionados.

Esta investigación concuerda con la conclusión de tesis (De Wit, 2013) que afirma que la preparación forense digital es un estado que permite estar listos para el análisis forense digital. El autor, además, concluye que a pesar de los motivos como el cumplimiento y el negocio en sí, para que las organizaciones busquen una preparación forense digital, las publicaciones sobre el tema son escazas. El experimentador concuerda con la escasez mencionada por De Wit, ya que al año en que se desarrolló la presente investigación, el tema de Preparación Forense Digital no tiene las referencias bibliográficas esperadas para un tema que el experimentador percibe como necesario, a excepción del libro “Implementing Digital Forensic Readiness” (Sachowski, J. y

Ivtchenko, D., 2016) que representa la unidad. Por otro lado, el experimentador considera que, dado que las organizaciones son lideradas por personas enfocadas en el desarrollo del negocio, es deber de los especialistas de tecnología de información, proponer un modelo que conlleve a la preparación forense digital a las organizaciones, para estar preparados para responder ante la necesidad de una investigación forense digital.

El aporte de una metodología (García Velásquez, 2014) para investigaciones de incidentes de seguridad informática, es un importante aporte que, sin embargo, nos tiene el enfoque proactivo de la presente investigación. La metodología propuesta ayuda a la investigación de un evento ocurrido en un medio informático, pero no toma en cuenta el problema del tiempo perdido por no recabar evidencia digital en las fuentes de evidencia críticas para el negocio y el impacto del consumo de recursos a la organización que este conlleva, sino que propone un método para realizar una investigación de computación forense. El plan de preparación forense digital, por su lado, permitió a la organización ganar tiempo valioso, al recolectar logs de sus equipos críticos, con un criterio centrado en el negocio, buscando la admisibilidad de la evidencia digital.

A pesar de no haber sido objeto de esta investigación, el experimentador concordó con la afirmación hecha tras el proyecto del autor (Morales Zamudio, 2010) sobre la criticidad de la aprobación de documentos para el éxito de un proyecto, en la medida que esto represente el apoyo de la alta gerencia a la implementación de una idea que traiga beneficios para la organización. Del mismo modo, el experimentador concuerda con la conclusión de Morales Zamudio (2010) quien afirma que el trabajo en

conjunto permite mitigar riesgos. Sin embargo, sobre la afirmación de Morales Zamudio, de no concentrarnos en quién tiene la culpa cuando sucede un incidente de seguridad informática el autor consideró necesario observar que la preparación forense digital debe colocarnos en una posición desde donde podamos ver los eventos y discernir si lo acontecido ha impactado el negocio de forma negativa para tomar las medidas correctivas que se crean convenientes. Esto es, la Computación Forense al servicio de la organización.

Tal como se espera de todo plan, el *Plan de Preparación Forense Digital*, propuso a la empresa tener un enfoque proactivo centrado en los riesgos del negocio para tener como resultado evidencia digital y gozar de un estado de preparación para enfrentar una investigación forense digital, así como capacitar y educar al personal sobre la criticidad de la evidencia digital en la Empresa. Los accidentes pasan, aunque no sepamos cuándo ni dónde. Así también debemos asimilar que llegará el momento en que necesitemos enfrentar un incidente de seguridad de información, y minimizar el riesgo que este representa en la organización. Mejorar la visibilidad de nuestras fuentes de evidencia es una estrategia que debe quedar incluida en la estrategia de gestión. Esto agiliza a toda organización que use tecnologías de información en su ambiente de producción.

VI. CONCLUSIONES Y RECOMENDACIONES

- ✓ La identificación y documentación de los equipos críticos en la Empresa fue posible a partir de la evaluación de riesgos para el negocio de la Empresa.

- ✓ Para asegurar la integridad de la evidencia digital, desde su nacimiento, hasta su eliminación, es necesario adecuar los controles administrativos, técnicos y físicos de la Empresa para que tenga un enfoque de preparación forense digital.

- ✓ La generación de reportes a partir de la evidencia digital recabada en las fuentes, fue posible a partir de la herramienta SIEM usada por la Empresa.

- ✓ Los reportes generados representan los eventos concretos registrados en un log u ocurridos en la fuente de evidencia digital.

- ✓ Definir qué eventos necesitamos monitorear en la fuente de evidencia digital, es un paso crítico para la generación de reportes.

- ✓ La capacidad de recabar evidencia digital en la empresa incrementó en un 68.35% en la Empresa, luego de elaborar e implementar el Plan de Preparación Forense Digital.

- ✓ La capacidad de recabar evidencia digital alcanza el 100% solo cuando el número de fuentes de evidencia digital identificadas es igual al número de fuentes de evidencia digital identificada y recabada.

- ✓ La capacidad negativa de recabar evidencia digital en la empresa disminuyo de 11.22% a 0%.

- ✓ El número total de fuentes de evidencia digital no identificada y recabada, siempre debe ser igual a cero, para que no exista un impacto negativo en el almacenamiento de la herramienta de recolección de logs.

- ✓ El Plan de Preparación Forense Digital permitió cumplir 96.88% de los sub requisitos del requerimiento 10 de PCI DSS versión 3.2.

- ✓ Es deber de los especialistas del área de gestión de riesgos en la empresa, proponer un modelo que conlleve a la preparación forense digital para poder responder a la necesidad de investigación forense digital, la cual es constante.

- ✓ El Plan de Preparación Forense Digital permitió a la Empresa ganar tiempo valioso, al recolectar logs de sus equipos críticos, con un criterio centrado en el negocio, buscando la admisibilidad de la evidencia digital.

Por otro lado, a partir de la presente investigación, el experimentador considera recomendable, para toda organización, los siguientes puntos:

- ✓ Realizar, como primer paso para la formulación de un plan de preparación forense digital, una evaluación de riesgo del negocio que permita identificar los escenarios de riesgo y las fuentes de evidencia digital asociadas.

- ✓ Utilizar una herramienta SIEM o mecanismo alternativo que centralice la recolección de logs de las fuentes de evidencia digital.

- ✓ Validar la existencia de un plan de respuesta en caso ocurra un incidente de seguridad en el que se requiera asegurar la fuente de evidencia digital, para protegerla de alteraciones que perjudiquen la investigación de los eventos, así como un futuro uso como evidencia digital ante una corte de justicia.

- ✓ Formar y educar en Forense Digital a equipos de Primera Respuesta, que estén conformados por personal que labore en horario rotativo de 24 horas los 7 días de la semana, así como por miembros de las áreas de Soporte de Tecnología de Información, Seguridad de Información y Seguridad Física.

- ✓ Ejecutar el Plan de manera anual y cada vez que ocurra un incidente de seguridad de información.

VII. REFERENCIAS BIBLIOGRÁFICAS

Barske D., Stander A. y Jordaan J. (2010). A Digital Forensic Readiness Framework for South African SME's. Recuperado el 22 de abril de 2016, de http://tinyurl.com/huvon3t

Cano Martinez, J. J. (2009). Computación forense. México, D.F.: Alfaomega.

Comisión de Fiscalización de Fiscalización de Barreras Comerciales no Arancelarias – INDECOPI . (2014). Norma Técnica Peruana NTP-ISO-IEC 27001:2014. Recuperado el 22 de abril de 2016, de http://tinyurl.com/zhd4ygo

De Wit, J. (2013). Continuous Forensic Readiness. Tesis de Maestría, Facultad de Ingeniería Eléctrica, Matemática y Ciencias de la Computación, Universidad de Twente. Twente, Paises Bajos.

García Velásquez, D. R. (2014). Metodología basada en el Cómputo Forense para la investigación de delitos informáticos. Tesis de grado, Escuela Profesional de Ingeniería en Computación, Facultad de Ingeniería, Universidad Nacional Autónoma de México. México D.F., México.

Gibson, D. (2016). SSCP Systems Security Certified Practitioner All-in-one exam guide (2da ed.). Nueva York: MC Graw Hill.

Grobler C. y Louwrens C. (2007). Digital Forensic Readiness as a Component of Information Security Best Practice. Recuperado el 22 de abril de 20016, de http://tinyurl.com/jozxd7c

International Council of E-Commerce Consultants. (2012). EC-Council Official Curriculum Certified Hacking Forensic Investigator Vol. 1. EC-Council.

ISACA. (2016). Cobit 5. Recuperado el 05 de mayo de 2016, de http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

Morales Zamudio, A. (2010). Diseño de una solución de un Sistema de Seguridad Informática en empresas estatales. Informe de suficiencia, Escuela Profesional de Ingeniería de Sistemas, Facultad de Ingeniería Industrial y de Sistemas, Universidad Nacional de Ingeniería. Lima, Perú.

Mouhtaropoulos A., Chang-Tsun L. y Grobler M. (2014). Digital Forensic Readiness: Are we there yet? Recuperado el 22 de abril de 2016, de http://tinyurl.com/h236epq

National Institute of Standards and Technology. (setiembre de 2012). SP 800 30 R1. Recuperado el 25 de abril de 2016, de http://tinyurl.com/h8lgalx

Palomino Pio, M. A. (2008). Mejora de los niveles de seguridad de información en las plataformas de sistemas – servidores. Informe de suficiencia, Escuela Profesional de Ingeniería de Sistemas, Facultad de Ingeniería Industrial y de Sistemas, Universidad Nacional de Ingeniería. Lima, Perú.

PC MAGAZINE. (2016). PC MAGAZINE. Recuperado el 20 de abril de 2016, de Sitio Web de PC Magazine: http://www.pcmag.com/encyclopedia/term/40169/computer-security

PCI Data Security Standar version 3.2. (abril de 2016). Recuperado el 2016, de http://tinyurl.com/z4a9msw

PCI SSC. (2016). Bienvenido al PCI Security Standards Council. Recuperado el mayo de 2016, de PCI SSC: https://es.pcisecuritystandards.org/minisite/en/

Rowlingson, R. (2004). A ten step process for Forensic Readiness. Recuperado el 21 de abril de 2016 , de International Journal of Digital Evidence: http://tinyurl.com/jfgo7nl

RSA Security Analytics Documentation: Home. (s.f.). Recuperado el 25 de abril de 2016, de https://tinyurl.com/zg4mly5

Sachowski, J. y Ivtchenko, D. (2016). Implementing digital forensic readiness. Cambridge, MA: Syngress.

Seytuque Limo, R. C. (2008). Desarrollo de un modelo de políticas de seguridad y gestión de TIC's aplicado al Gobierno Regional Lambayeque. Tesis de grado, Escuela Profesional de Ingeniería en Computación e Informática, Facultad de Ciencias Físicas y Matemáticas, UNPRG. Lambayeque, Perú.

Sule, D. (2014). Importance of Forensic Readiness . Recuperado el 25 de abril de 2016, de ISACA JOURNAL: http://tinyurl.com/gtrlezx

Superintendencia de Banca, Seguros y AFP. (2009). Circular N° G-140-2009. Recuperado el 22 de abril de 2016, de http://tinyurl.com/gr55q59

Tan, J. (2001). Forensic Readiness. Recuperado el 22 de abril de 2016, de http://tinyurl.com/zgb3x3a

Vallejos Saravia, B. A., & Suyon Urquizo, J. A. (2010). Desarrollo de un Plan de Riesgo de Tecnología de la Información para la Sub-Gerencia de Racionalización e Informática de la Sede del Gobierno Lambayeque, utilizando Metodología Magerit. Tesis de grado, Escuela Profesional de Ingeniería en Computación e Informática, Facultad de Ciencias Físicas y Matemáticas, UNPRG. Lambayeque, Perú.

VIII. ANEXOS

8.1 Plan de Preparación Forense Digital, elaborado para la Empresa

Título del Documento: *Plan de Preparación Forense Digital*
Tipo: Plan
Hoja de Control de cambios: Sí
Tabla de Contenidos: Sí
Introducción: Sí
Objetivos: Sí Detalle: • *Maximizar la capacidad de recolectar evidencia digital en la Empresa.* • *Minimizar el costo de investigación de un incidente de seguridad.*
Definiciones: Sí
Justificación: Sí Detalle: *Estar preparados para responder ante una investigación forense digital de un evento de seguridad dentro de la empresa, como pueden ser: la violación de las políticas de seguridad de información o el quebrantamiento de las leyes peruanas, usando nuestros recursos tecnológicos.*
Alcance: Sí Detalle: *Este plan abarca toda la infraestructura tecnológica usada por la Empresa que puede generar evidencia digital de las acciones de los usuarios y que es considerada crítica por el análisis de riesgo del negocio.*
Definición de Preparación Forense Digital: Sí Detalle: *El concepto de Preparación Forense Digital fue acuñado por John Tan (2001). Según el Dr. Robert Rowlingson (2004), visto desde una perspectiva empresarial, la preparación forense digital es la habilidad de una organización para maximizar su potencial para usar evidencia digital cuando esta sea requerida. Esto implica poder utilizar los recursos de la empresa, en su beneficio, para minimizar los costos de investigación cuando ocurra un incidente de seguridad o un evento concreto.* *El presente plan se compone de los siguientes pasos, los mismos que deben ser evaluados de manera anual, por la Gerencia de Riesgos, y cuyo resultado debe ser usado a favor de la Empresa y de sus beneficiarios.* *1.- Definir los escenarios de riesgo para el negocio* *Se debe reconocer, mediante una evaluación de riesgo, el impacto potencial para el negocio de la Empresa, desde varios tipos de crímenes digitales, incidentes o eventos. Esta evaluación de riesgo describe desde la perspectiva*

del negocio, dónde se requiere evidencia digital y sus beneficios para la reducción del impacto en el negocio. Este debe ser el aspecto más crítico en cuanto a la práctica de la preparación forense digital en la Empresa.

2.- Identificar las fuentes de evidencia digital disponibles

Es sumamente importante la documentación de las fuentes de evidencia digital disponibles. Debemos identificar nuestras fuentes de evidencia digital y aquellos recursos en donde la evidencia digital no se está generando de forma apropiada, para corregir y alinear.

3.- Definir los requisitos para la recolección de evidencia digital

Enfocar la atención en los requisitos para la recolección de evidencia digital en las fuentes de evidencia identificadas en soporte de todos los escenarios de negocio que apliquen. De esta forma será posible que la Gerencia de Riesgo pueda comunicar cuáles son los requisitos y distribuirlos a los equipos de soporte necesarios para la implementación. Debe de considerarse aspectos como el almacenamiento seguro de la evidencia digital de modo que se proteja su integridad, disponibilidad y confidencialidad.

4.- Establecer la admisibilidad legal de la evidencia digital

Luego de haber identificado nuestras fuentes, basados en la evidencia digital relevante para mitigar los riesgos de negocio conocidos y de haber comprendido y documentado los requisitos para la recolección de evidencia, debemos implementar mecanismos para probar su autenticidad, usando controles administrativos, técnicos y físicos, así como también, para preservarla. En este punto es necesario que la empresa cuente con la asesoría legal que garantice el carácter admisible de la evidencia digital recolectada.

5.- Establecer un almacenamiento y manipulación seguros

Cuando la evidencia digital sea preservada en almacenamiento de largo plazo o que no se encuentre en línea (data en descanso), debe hacerse de manera muy segura, y debe estar disponible cuando se la requiera. Sin importar la opción de almacenamiento elegida, se debe mantener la autenticidad, confidencialidad e integridad, y su disponibilidad inmediata. La Política de Seguridad de Información de la empresa debe garantizar la viabilidad de la práctica forense digital desde la creación de la data, de modo que se garantice la admisibilidad legal de la evidencia digital durante su eventual manejo y almacenamiento.

6.- Habilitar el monitoreo dirigido

Debemos monitorear las fuentes de evidencias directas que proveen contexto a los escenarios de riesgo identificados, de modo que podamos identificar y detectar los eventos antes de que se transformen en incidentes de seguridad.

7.- Definir flujos de investigación

Todos los eventos sospechosos detectados dentro de la infraestructura tecnológica de la empresa, deben ser revisados para determinar el impacto y potencial riesgo para las operaciones del negocio. Según sea el nivel de riesgo identificado, deberá decidirse cómo se manejará dicho incidente, en concordancia con el plan de respuesta a incidentes definido en la Empresa.

8.- Implantar la educación continua

Todo el personal de la organización que participe en la respuesta a un incidente o investigación, debe ser capacitado, según sea su rol, de modo que tenga el conocimiento necesario para llevar a cabo su función.

9- Formular informes de investigación, basados en la evidencia digital

Puesto que uno de los objetivos para ejecutar cualquier investigación es la de usar evidencia digital como una manera de obtener respuesta a preguntas acerca de un incidente o evento, demostrando credibilidad, debemos presentar las conclusiones basándonos en evidencia plasmada en reportes.

10.- Asegurar la revisión legal

Debemos contar con el apoyo de un Asesor Legal para la revisión de los asuntos asociados a la evidencia digital, desde el punto de vista del Derecho Civi y Penal cuya opinión experta acredite la evidencia digital generada en nuestra organización.

8.2 Resultados de la implementación del Plan

A continuación se detallan las acciones llevadas a cabo para la implementación del Plan de Preparación Forense Digital en la Empresa:

Paso	Acciones	Impacto	Madurez
1	Se identificó el riesgo del negocio "Incumplimiento de la norma PCI DSS" Información sobre la aplicabilidad de PCI DSS: La PCI DSS se aplica a todas las entidades que participan en el procesamiento de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios. La PCI DSS se aplica a todas las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta y/o datos confidenciales de autenticación.	Alto	Alta
2	Se creó el documento (.xls) matriz, llamado "Fuentes de Evidencia Digital versión 16.01", donde se define el alcance de equipos afectados por el análisis de riesgo de negocio y que deben ser monitoreados por la herramienta SIEM de la empresa. El documento creado en MS Excel, se compone de: Hoja 1: "Servidores" Columnas: Nombre de host: Dirección IP: Tipo: Servidor, Dispositivo (appliance) Hardware: Sistema Operativo: SW Base: Función: Grupo: (De aplicaciones) Enganchado: Sí, No. Envio de logs: Sí, No. Reportes: Sí, No. Alarmas: Sí, No. Hoja 2: "Equipos de comunicaciones"	Alto	Alta

	Columnas: Ubicación física: Descripción: Marca: Modelo: Serie: Versión: Tipo: Simple, Nodo 1, Nodo 2, etc. IP: IP virtual: Enganchado: Sí, No. Envio de logs: Sí, No. Parser: Sí, No. Reportes: Sí, No. Alarmas: Sí, No.		
3	3.1 Control administrativo: Se modificó la **Política de Seguridad de Información** de la empresa, agregando el inciso 12.5.6.1 Recolección de evidencia digital, el cual indica: *Existen dos escenarios diferenciables para la recolección de evidencia.* *1) La evidencia digital, generada a partir de logs, es enviada en línea hacia la herramienta de recolección, para un análisis centralizado.* *2) La evidencia digital debe ser recolectada in situ, con la autorización de la Gerencia de Riesgos o por una orden judicial, bajo la asesoría del asesor legal de la Empresa.* *Para el primer caso, los requisitos de colección de evidencia son:* • *El almacenamiento de la evidencia digital debe ser de forma centralizada, en un equipo dedicado para la recolección de logs.* • *La evidencia digital almacenada debe ser respaldada de manera diferencial y diaria.*	Alta	Media

	Para el segundo caso, los requisitos de colección de evidencia se especifican en el Plan de Respuesta a Incidentes definidos por la Empresa. *El acceso físico el acceso físico a la herramienta SIEM está restringido y solo puede ser autorizado por la Gerencia de Riesgo, la Gerencia de Tecnología o la Gerencia General.*		
	3.2 Control administrativo: Se modificó el **Plan de Respuesta a Incidentes** de la empresa, agregando el inciso *6.2 Recolección de evidencia digital in situ*, el cual indica: *Cuando la evidencia digital deba ser recolectada in situ, con la autorización de la Gerencia de Riesgos o por una orden judicial, bajo la asesoría del asesor legal de la Empresa, se deben seguir los siguientes pasos:* • *El personal miembro del Equipo de Primera Respuesta deberá acudir a la escena en donde se encuentra el dispositivo cuya evidencia digital necesitamos capturar.* • *Una vez en la escena:* o *No manipular el equipo.* o *No desconectar el equipo de la fuente de energía eléctrica.* o *Desconectar el cable de red.* o *Cercar el lugar hasta el arribo del personal Forense Digital (consultor externo), para iniciar el proceso de investigación forense digital.* Además, se agregó el punto 7 Equipo de Primera Respuesta, el cual dice: *El Equipo de Primera Respuesta, será el encargado de acudir a la escena de un delito informático dentro de las instalaciones de la Empresa* *Está conformado por los siguientes*	Alta	Media

	colaboradores: • *Personal de Soporte de TI.* • *Personal de Seguridad de Información.* • *Operadores de Producción.* • *Personal de Seguridad Física.*		
	3.3 Control técnico: Se configuró la herramienta SIEM para que las cuentas de usuarios con acceso a este sistema, tengan asignado un rol que tenga asignado solo los privilegios necesarios para realizar su función.	Alta	Alta
	3.4 Control físico: En cumplimiento de la Política de Seguridad de la Información, el acceso físico a la herramienta SIEM está restringido y solo puede ser autorizado por la Gerencia de Riesgo, la Gerencia de Tecnología o la Gerencia General. El equipo se encuentra en un área de alta seguridad, con circuito cerrado de televisión, y exclusas cuyas puertas solo se abren mediante una tarjeta de proximidad autorizada, las mismas que son otorgadas por el personal de seguridad física, al visitante, posterior a su identificación y autorización. El acceso físico al área en donde se encuentra el equipo, se documenta en el cuaderno de registro, considerando los siguientes datos: • Fecha de visita • Hora de entrada • Hora de salida • Nombre del visitante. • Empresa a la que pertenece. • Motivo • Firma	Alta	Alta
4	4.1 Control administrativo: Se modificó la **Política de Seguridad de Información** de la empresa, agregando el inciso 12.5.6.2 Admisibilidad de la evidencia digital, el cual indica: *El Asesor Legal de la Empresa será*	Alto	Media

	convocado para participar de la revisión de la evidencia digital recabada en la empresa, por lo menos una vez año, o ante la ocurrencia de un incidente de seguridad que demande la intervención de un especialista Forense Digital.		
5	5.1 Control Administrativo Se modificó la **Política de Seguridad de Información** de la empresa, agregando el inciso 12.5.6.3 Almacenamiento y manipulación de la evidencia digital, el cual indica: *La evidencia digital recabada en la herramienta SIEM de la Empresa, debe tener una copia de respaldo, cuya integridad debe ser validada con el uso de una herramienta de monitoreo de integridad, según lo especificado en el inciso 6.3 del Plan de respuesta a incidentes.* *La Empresa espera que la evidencia recolectada en una escena de delito informático por el consultor externo especialista en Investigaciones Forenses Digitales, siga los procedimientos científicos de la computación forense. Debe de estar presente el Asesor Legal de la Empresa. La evidencia digital debe de estar acompañada por el documento Cadena de Custodia, en donde se documente las acciones llevadas a cabo sobre la evidencia digital para luego poder der almacenada.* *El intervalo de tiempo o antigüedad mínima de la evidencia digital, para su almacenamiento externo, es de un año a partir de la fecha de su creación. Antes de almacenar en un medio externo el archivo que contiene la evidencia digital, debe ejecutarse un programa para la generación de un valor HASH también llamado "suma de verificación" sobre el archivo, que permita validar la integridad de la*	Alto	Alta

	evidencia. El valor obtenido debe ser documentado y almacenado con la evidencia digital. *El intervalo de tiempo o antigüedad mínima de la evidencia digital, para ser considerada no necesaria, y proceder con su eliminación es de 05 años y debe contar con la aprobación de la Gerencia de Riesgo, Auditoría Interna, siguiendo los procedimientos establecidos para la eliminación de medios de almacenamiento.*		
6	6.1 Control Técnico: Las fuentes de evidencia digital, identificadas y recabadas, envían logs a la herramienta SIEM usada por la Empresa, adquirida en el año 2016. Esta herramienta tiene la función de correlacionar eventos, lo que le permite generar alertas en tiempo real cuando correlaciona dos o más eventos sospechosos en los equipos monitoreados, como por ejemplo, cuando un código de usuario falla al intentar iniciar sesión en un equipo, pero logra iniciar sesión en otro (posible ataque de fuerza bruta).	Alta	Media
7	7.1 Control Administrativo El Procedimiento de Monitoreo de Eventos de Seguridad, de la Empresa, ya establece la revisión diaria de los reportes generados por la herramienta SIEM.	Alta	Alta
	7.2 Control Administrativo El Plan de Respuesta a Incidentes presenta un flujo-grama donde se especifica cómo interactúan las partes que reportan el incidente y los receptores del mensaje y qué acciones llevan a cabo estos. Se modificó el Flujo-grama, de manera que: • El proceso de investigación se inicia con el análisis de eventos en la herramienta SIEM de la empresa, o a solicitud de un área usuaria de la Empresa. • El personal designado por la Gerencia de Riesgo realiza un análisis de impacto de los eventos analizados, basado en tres	Alta	Media

	categorías: o Bajo: Hacer seguimiento al evento. La formulación de un informe no es necesaria para estos eventos. o Medio: Iniciar una investigación del evento, con un informe, basado en reportes. o Alto: La investigación del evento debe de ser hecha por el equipo de Riesgos y por el equipo Forense Digital del consultor externo, en coordinación con el Asesor Legal de la Empresa.		
8	8.1 Control Administrativo: Se modificó la **Política de Seguridad de Información** de la empresa, agregando el inciso 12.5.6.4 Capacitación, el cual indica: *Los miembros del Equipo de Primera Respuesta deberán ser capacitados por lo menos una vez al año, por un experto Forense Digital, certificado, para poder atender un incidente informático que requiera de conocimientos básicos para proteger la evidencia digital de cualquier alteración no deseada.*	Media	Alta
9	9.1 Control Administrativo Se modificó la **Política de Seguridad de Información** de la empresa, agregando el inciso 12.5.6.5 Informes de Investigación, el cual indica: *Toda investigación llevada a cabo por el personal de la Gerencia de Riesgo, usando los recursos de la Empresa, debe de presentar un Informe de Investigación enfocado específicamente en los hechos descubiertos durante la investigación. El informe de investigación será considerado relevante y creíble, siempre y cuando sean una representación precisa de los eventos, independientemente si la evidencia digital demuestra culpa o inocencia.*	Alta	Media
	9.1 Control Técnico	Alta	Alta

	Se configuraron reportes en los equipos seleccionados en la muestra, como se indica a continuación: • Equipo: Controlador de Dominio (10) o Usuario creado o Usuario eliminado o Usuario bloqueado o Usuario desbloqueado o Usuario inhabilitado o Usuario habilitado o Usuario agregado a grupo o Usuario retirado de grupo o Logueo fallido o Contraseña establecida • Equipo: Anti Spam o Logueo exitoso o Logueo fallido o Cambios en configuración • Equipo: Anti Virus o Logueo exitoso o Logueo fallido o Cambios en configuración • Equipo: IPS o Usuario creado o Usuario eliminado o Usuario modificado o Logueo exitoso o Logueo fallido		
10	La Empresa cuenta con el apoyo de un Abogado Civil y un Abogado Penal, a disposición, quienes pueden brindar la asesoría legal necesaria.	Alto	Medio

8.3 Soporte al requisito 10 de la norma PCI DSS

El requisito número 10 de PCI DSS declara: "Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta". El plan de preparación forense digital es un soporte para el cumplimiento de este requerimiento.

Requisito	Descripción	PPFD
10.1	Implemente pistas de auditoría para vincular todo acceso a componentes del sistema con usuarios específicos.	Paso 03
10.2	Implemente pistas de auditoría automáticas en todos los componentes del sistema a fin de reconstruir los siguientes eventos:	Paso 03
10.2.1	Todo acceso por parte de usuarios a los datos del titular de la tarjeta.	Paso 03
10.2.2	Todas las acciones realizadas por personas con privilegios de raíz o administrativos	Paso 03
10.2.3	Acceso a todas las pistas de auditoría	Paso 03
10.2.4	Intentos de acceso lógico no válidos	Paso 03
10.2.5	Uso y cambios de los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y el aumento de privilegios, y de todos los cambios, incorporaciones y eliminaciones de las cuentas con privilegios administrativos o de raíz.	Paso 03
10.2.6	Inicialización, detención o pausa de los registros de auditoría	Paso 03
10.2.7	Creación y eliminación de objetos en el nivel del sistema	Paso 03
10.3	Registre, al menos, las siguientes entradas de pistas de auditoría de los componentes del sistema para cada evento:	Paso 03
10.3.1	Identificación de usuarios	Paso 03
10.3.2	Tipo de evento	Paso 03
10.3.3	Fecha y hora	Paso 03
10.3.4	Indicación de éxito o fallo	Paso 03
10.3.5	Origen del evento	Paso 03
10.3.6	Identidad o nombre de los datos, componentes del sistema o recursos afectados.	Paso 03
10.4	Utilizando tecnología de sincronización, sincronice todos los tiempos y relojes críticos y asegúrese de que lo siguiente sea implementado para adquirir, distribuir y almacenar tiempos	Paso 03
10.4.1	Los sistemas críticos tienen un horario uniforme y correcto.	Paso 03
10.4.2	Los datos de tiempo están protegidos.	Paso 03
10.4.3	Los parámetros de la hora se reciben de fuentes aceptadas	Paso 03

	por la industria.	
10.5	Proteja las pistas de auditoría para que no se puedan modificar.	Paso 05
10.5.1	Limite la visualización de las pistas de auditoría a quienes lo necesiten por motivos laborales.	Paso 05
10.5.2	Proteja los archivos de las pistas de auditoría contra modificaciones no autorizadas.	Paso 05
10.5.3	Realice copias de seguridad de los archivos de las pistas de auditoría de manera oportuna en medios o servidores de registros centralizados que sean difíciles de modificar.	Paso 05
10.5.4	Elabore registros para tecnologías externas en un dispositivo de medios o un servidor de registros interno, seguro y centralizado.	Paso 05
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 agregar nuevos datos no deba generar una alerta).	Paso 05
10.6	Revise los registros y los eventos de seguridad en todos los componentes del sistema para identificar anomalías o actividades sospechosas.	Paso 06
10.6.1	Revise las siguientes opciones, al menos, una vez al día: ✓ Todos los eventos de seguridad. ✓ Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD ✓ Registros de todos los componentes críticos del sistema. ✓ Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, firewalls, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención], servidores de autenticación, servidores de re-direccionamiento de comercio electrónico, etc.).	Paso 06
10.6.2	Revise los registros de todos los demás componentes del sistema periódicamente, de conformidad con la política y la estrategia de gestión de riesgos de la organización y según lo especificado en la evaluación anual de riesgos de la organización.	Paso 06
10.6.3	Realice un seguimiento de las excepciones y anomalías	Paso 06

	detectadas en el proceso de revisión.	
10.7	Conserve el historial de pistas de auditorías durante, al menos, un año, con un mínimo de disponibilidad para análisis de tres meses (por ejemplo, en línea, archivados o recuperables para la realización de copias de seguridad).	Paso 05
10.8	Requisitos adicionales solo para los proveedores de servicios: Implementar un proceso para la detección oportuna y la presentación de informes de fallas de los sistemas críticos de control de seguridad, incluido pero no limitado a la falla de: ✓ Firewalls ✓ IDS/IPS ✓ FIM ✓ Antivirus ✓ Controles de acceso físicos ✓ Controles de acceso lógico ✓ Mecanismos de registro de auditoría ✓ Controles de segmentación (si se utilizan)	Paso 09
10.8.1	Requisitos adicionales solo para los proveedores de servicios: Responder a las fallas de los controles de seguridad críticos en el momento oportuno. Los procesos para responder en caso de fallas en el control de seguridad son los siguientes: ✓ Restaurar las funciones de seguridad ✓ Identificar y documentar la duración (fecha y hora de inicio a fin) de la falla de seguridad ✓ Identificar y documentar las causas de la falla, incluida la causa raíz, y documentar la remediación requerida para abordar la causa raíz ✓ Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad. ✓ Realizar una evaluación de riesgos para determinar si se requieren más acciones como resultado de la falla de seguridad ✓ Implementar controles para prevenir que se vuelva a producir la causa de la falla ✓ Reanudar la supervisión de los controles de seguridad	No aplica
10.9	Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear todos los	No aplica

	accesos a los recursos de la red y a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.

8.4 Herramienta SIEM "Security Analytics"

Security Analytics es un SIEM del fabricante RSA, quién ha reemplazado al predecesor "enVision" con esta potente herramienta. En el portal de la marca RSA (RSA Security Analytics Documentation: Home), Security Analytics es definido de la siguiente manera:

> *"RSA Security Analytics es una solución de seguridad que aprovecha la tecnología comprobada de los componentes de RSA Core para ofrecer monitoreo de seguridad de la red, información de seguridad centralizada y administración de eventos (SIEM) de manera convergente. A diferencia de las soluciones de seguridad basadas en firmas o perímetros, RSA Security Analytics ayuda a los analistas a descubrir comportamiento "interesante" o "anómalo" sin depender del conocimiento previo sobre las herramientas o las técnicas específicas de los atacantes.*
>
> *La plataforma visual unifica la analítica de seguridad, como la detección, la investigación, la generación de informes y el contenido y la administración en una única interfaz basada en navegador. La arquitectura está diseñada para reunir otras tecnologías de seguridad, como la combinación del tráfico de red y los datos de eventos de registro, para proporcionar los análisis de centro de operaciones de seguridad más eficaces y eficientes."*

8.5 Costos del SIEM "Securty Analytics"

La siguiente tabla muestra el costo de licenciamiento de la herramienta SIEM que lleva por nombre "Security Analytics" versión 10.5, del fabricante RSA. El precio es en dólares americanos. La columna "Cant." (cantidad) representa el número de meses dentro del licenciamiento.

Fecha: 22/02/2016

Item	Marca	Descripción	Cant.	Precio Total
1	RSA	Series 4S Analytics Svr 10U BscMnt1M	12	$ 4,873.12
2		S5SHeadUnit EvntSrmAnalysis B.	12	$ 5,696.00
3		Series 5 Hybrid for Logs BscMnt1M	12	$ 7,344.00
4		22TB HD DAC 4Log Hybrid w/lic B.	12	$ 3,968.00
Sub Total (US$)				$ 21,881.12
IGV (US$)				$ 3,938.60
Total (US$)				$ 25,819.72

Tabla 11: Costos del SIEM