EDP UNIVERSITY DE PUERTO RICO, INC.

RECINTO DE HATO REY

PROGRAMA DE MAESTRÍA EN SISTEMAS DE INFORMACIÓN

ESPECIALIDAD EN SEGURIDAD DE INFORMACIÓN

E INVESTIGACIÓN DE FRAUDE

Víctimas de Robo de Identidad por ataque a Sony Pictures Entertainment Inc.

ANÁLISIS DE CASO: MICHAEL CORONA & CHRISTINA MATHIS VS. SONY PICTURES ENTERTAINMENT, INC.

Número de Caso: 2:14-cv-09600-RGK-E

REQUISITO PARA LA MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Especialidad en Seguridad de Información e Investigación de Fraude

Septiembre 2018

Josué Omar Rivera Morales

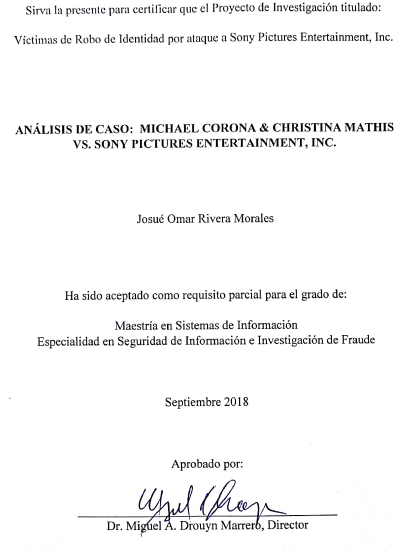


TABLA DE CONTENIDO

SECCIÓN 1: INTRODUCCIÓN Y TRASFONDO 1

Introducción 1

Trasfondo del caso 6

Descripción de hechos 9

Acusaciones, cargos y términos 12

Definición de términos 14

SECCIÓN 2: REVISIÓN DE LITERATURA 16

Introducción 16

Leyes aplicables 18

Casos relacionados 22

SECCIÓN 3: SIMULACIÓN 25

SECCIÓN 4: INFORME DEL CASO 35

Resumen ejecutivo 35

Objetivo 35

Alcance del trabajo 36

Datos del caso 36

Descripción de los dispositivos utilizados 36

Resumen de hallazgos 37

Cadena de custodia 37

Procedimiento 40

Conclusión 47

SECCIÓN 5: DISCUSIÓN DEL CASO 48

SECCIÓN 6: AUDITORÍA Y PREVENCIÓN 49

SECCIÓN 7: CONCLUSIÓN 52

SECCIÓN 8: REFERENCIAS 52

TABLA DE FIGURAS

Página

Figura 1. Estadísticas de robo de información 16

Figura 2. Acceso al sistema, cuenta administradora 24

Figura 3. Primera conexión de los hackers de instalación de archivos 24

Figura 4. Instalación del malware al sistema 25

Figura 5. Aviso de los hackers luego de instalar malware al sistema 25

Figura 6. Primera exposición de archivos al público 26

Figura 7. Contraseñas de empleados expuestas al público 26

Figura 8. Exposición de documentos financieros de la compañía y empleados 27

Figura 9. Segundo comunicado de los hackers utilizando la página “Pastebin” 27

Figura 10. Cuenta de Outlook de Amy Pascal, Co-Director de Sony en el ataque 28

Figura 11. Comunicado de los hackers a través del email de Amy Pascal 29

Figura 12. Comunicado por parte de GOP en el sistema 29

Figura 13. Archivos difundidos por los hackers 30

Figura 14. Comunicado de los hackers por la página “Pastebin” 31

Figura 15. Comunicado por los hackers 31

Figura 16. Lista de archivos expuestos 32

Figura 17. Comunicado de los hackers en el sistema 33

Figura 18. Comunicado de GOP a través del sistema de la compañía 33

Figura 19. Último comunicado de GOP 34

Figura 20. Página principal para el comienzo del análisis 40

Figura 21. Fuente de evidencia del USB 41

Figura 22: Preparación de archivos para analizar el caso 41

Figura 23. Creación de la imagen 42

Figura 24. Documentos y archivos sobre los exempleados 42

Figura 25. Información personal de los demandantes difundida al público 43

Figura 26. Cartas de renuncia de las demandantes expuestas por los hackers 44

Figura 27. Itinerario de citas médicas expuesto 45

Figura 28. Informes sobre planes de retiro 46

**SECCIÓN 1: INTRODUCCIÓN Y TRASFONDO DEL CASO**

**Introducción**

El presente trabajo estará basando en el hurto de identidad, fraude cibernético. Por lo general, debemos entender que hoy en día la mayoría de todas las diligencias que se hacen a diario de cierta forma están relacionadas con la tecnología. Los dispositivos tecnológicos como el celular, la computadora, agendas digitales y un sin fin de equipos que se posee guardan o retienen información privada de las personas. Esto, de cierta manera también incluye las tarjetas de crédito, visas y pasaportes, entre otros documentos que a través del tiempo han sido actualizados a través del uso de la tecnología. La vulnerabilidad en lo que son las tarjetas de crédito visas y pasaportes, entre otros documentos es muy alta, ya que la mayoría de estos estos no tan solo contienen información personal, sino que también incluyen información muy sensitiva como lo es el número de seguro social o, tal vez algún número de empleado, entre otros.

De otra parte, diariamente muchísimas compañías en nuestro país y alrededor del mundo, son demandadas por el hurto de información personal o mejor conocido como el robo de identidad. Según Merritt (2016) “la Comisión Federal de Comercio recibió más de 250,000 reclamaciones de identidades robadas.”

De acuerdo con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) (2017) señalan que para el 2016 se registraron más de 1,765,654 de reclamaciones en el sector bancario, sobrepasando el número de reclamaciones registradas para el 2015. Estos datos nos llevan a deducir que el robo de información es uno de los problemas que más impacta a los consumidores día tras día. Dado que todo está relacionado con la tecnología, la parte perjudicial no es solo el hurto de la información personal, sino más importante aún es lo que puede hacer la persona que tenga esta información. Es este aspecto en que la mayoría de los fraudes son cometidos tanto con las tarjetas de crédito como estafas de diferentes maneras. Muchos de estas personas buscan las vulnerabilidades de los sistemas de información para obtener diferentes tipos de información o documentación necesaria para lograr su objetivo. Las agencias de créditos y bancos poseen sistemas muy grandes de almacenaje de información, lo que los convierte en un blanco de ataque, convirtiéndose en espacios únicos para que surjan fraudes cibernéticos. Las personas buscan engañar, y hacen uso de varios métodos como *phishing, pharming* y *spam,* entre otras.

El *phishing* es una de las estrategias más conocidas. También se le conoce como suplantación de identidad, en esta estrategia la persona que realiza el robo se le conoce como *phisher*. El phishing se hace pasar por una persona o una empresa de confianza mediante hacer una comunicación oficial a través de redes sociales, mensajería instantánea y por lo general a través de un correo electrónico. De esta manera la persona que está siendo víctima de robo no dudaría en suministrar la información requerida por el phishing y a su vez el phishing logra hacer el robo de información. En el caso del *pharming*, surge a través de un enlace (link), el cual redirige a la persona a una página fraudulenta, en la que se comente el fraude. El *spam*es mejor conocido como el correo electrónico basura, ya que la mayoría de los correos electrónicos que entran a este correo son páginas con virus que, al abrirlas, liberan el virus, lo que facilita el acceso a los dispositivos de las personas.

No obstante, hay muchas maneras de evitar estos problemas, se deben comenzar por estudiar y evaluar la estructura de los sistemas de información y seguridad de las diferentes compañías, organizaciones o agencias que trabajan con información sensitiva y que se pueden convertir en atracción para cometer este tipo de fraude. Ya evaluado los sistemas de información y de seguridad y luego de hacer los ajustes que sean necesarios para un mejor funcionamiento. Las personas juegan una parte muy importante en todo este dilema ya que los consumidores, empleados y personal debe mantenerse continuamente al tanto sobre la información que brindan a las diferentes entidades, bancos y lugares que requiera utilizar la información personal. Se debe tomar en consideración la versatilidad de las personas que se dedican a realizar estos robos, ya que muchas de estas personas buscan la forma más sencilla de estafar a las personas, y de las formas más sanas que se puede imaginar una persona, como por ejemplo una llamada telefónica. El robo de identidad no solo hace que las víctimas lleguen a tener problemas económicos, sino que también puede afectar su reputación y pueden afectarse psicológicamente de una manera que trasciende a nivel social. También hace que muchas personas víctimas del robo pierdan la credibilidad antes sus empleadores, sean expulsados de sus escuelas y/o universidades, tengan litigios legales, entre muchas otras situaciones.

En fin, el robo de información personal es uno de mucha controversia. Se debe mantener al tanto de todo documento y se debe ser muy cauteloso dónde a quiénes se le brinda información. La causa y el interés para realizar el trabajo sobre este tema es que cualquier persona puede estar susceptible a este problema. El objetivo principal de esta investigación es estudiar los diferentes tipos de fraude y crímenes informáticos, mediante educar y llevar al lector una visión clara de lo que sucede diariamente y lo que tiene origen en las redes. A su vez, se presentarán las diferentes formas y procedimientos que se deben realizar para que las compañías puedan tener un mejor servicio de seguridad y de sistemas de información.

**Descripción de caso**

Número de Caso:

2:14-cv-09600-RGK-E

Partes del caso:

**Demandante:** Michael Corona & Christina Mathis

**Acusado:** Sony Pictures Entertainment, Inc.

**Abogados:**

**Michael Corona representado por:**

Daniel C. Girard, [Girard Gibbs LLP](https://www.law360.com/firms/girard-gibbs)

Gretchen Freeman Cappio, [Keller Rohrback LLP](https://www.law360.com/firms/keller-rohrback)

Khesraw Karmand, [Keller Rohrback LLP](https://www.law360.com/firms/keller-rohrback)

Cari C. Laufenberg, [Keller Rohrback LLP](https://www.law360.com/firms/keller-rohrback)

Matthew J. Preusch, [Keller Rohrback LLP](https://www.law360.com/firms/keller-rohrback)

Lynn L. Sarko, [Keller Rohrback LLP](https://www.law360.com/firms/keller-rohrback)

Katrina Carroll, [Lite DePalma Greenberg LLC](https://www.law360.com/firms/lite-depalma)

Kyle A. Shamberg, [Lite DePalma Greenberg LLC](https://www.law360.com/firms/lite-depalma)

Roger Norton Heller, [Lieff Cabraser Heimann & Bernstein LLP](https://www.law360.com/firms/lieff-cabraser)

**Christina Mathis Representada por:**

Daniel C. Girard, [Girard Gibbs LLP](https://www.law360.com/firms/girard-gibbs)

Cari C. Laufenberg, [Keller Rohrback LLP](https://www.law360.com/firms/keller-rohrback)

Matthew J. Preusch, [Keller Rohrback LLP](https://www.law360.com/firms/keller-rohrback)

Gretchen Freeman Cappio, [Keller Rohrback LLP](https://www.law360.com/firms/keller-rohrback)

Lynn L. Sarko, [Keller Rohrback LLP](https://www.law360.com/firms/keller-rohrback)

Khesraw Karmand, [Keller Rohrback LLP](https://www.law360.com/firms/keller-rohrback)

Katrina Carroll, [Lite DePalma Greenberg LLC](https://www.law360.com/firms/lite-depalma)

Kyle A., Shamberg, [Lite DePalma Greenberg LLC](https://www.law360.com/firms/lite-depalma)

Roger Norton Heller, [Lieff Cabraser Heimann & Bernstein LLP](https://www.law360.com/firms/lieff-cabraser)

**Sony Pictures Entertainment, Inc. representado por:**

Michael J. Bayer, [Wilmer Cutler Pickering Hale and Dorr LLP](https://www.law360.com/firms/wilmerhale)

Andrew S. Dulberg, [Wilmer Cutler Pickering Hale and Dorr LLP](https://www.law360.com/firms/wilmerhale)

William F. Lee, Wilmer Cutler Pickering Hale and Dorr LLP

Noah A. Levine, [Wilmer Cutler Pickering Hale and Dorr LLP](https://www.law360.com/firms/wilmerhale)

David C. Marcus, [Wilmer Cutler Pickering Hale and Dorr LLP](https://www.law360.com/firms/wilmerhale)

Colin Reardon, Wilmer Cutler Pickering Hale and Dorr LLP

Alan E. Schoenfeld, [Wilmer Cutler Pickering Hale and Dorr LLP](https://www.law360.com/firms/wilmerhale)

Felicia H. Ellsworth, [Wilmer Cutler Pickering Hale and Dorr LLP](https://www.law360.com/firms/wilmerhale)

Christopher Thomas Casamassima, [Wilmer Cutler Pickering Hale and Dorr LLP](https://www.law360.com/firms/wilmerhale)

**Jueces:**

R. Gary Klausner, de la Corte del Distrito de California Central.

**Trasfondo del caso**

La queja principal de los demandantes va dirigida a lo que tiene que ver relacionado con el robo de identidad y todo lo relacionado a esto. La denuncia principal se crea debido a que los demandantes fueron afectados de manera directa cuando la compañía Sony Pictures Entertainment, Inc., fue saqueada cibernéticamente por el grupo de hackers Guardians of Peace mejor conocidos como “GOP”. Estos tuvieron la oportunidad de robar más de 25 gigabytes de información tales como: dirección, números de teléfono, números de seguridad social e información médica y salarial, cartas de renuncias, etc. sobre empleados de Sony. Esta demanda o denuncia fue generada por Michael Corona y Christina Mathis, ambos ex-empleados de la compañía Sony Pictures Entertainment, Inc. Michael fue empleado por Sony desde el 2004 hasta el 2007 en el estado de California. Por otro lado, la demandante Christina Mathis fue contratada por una compañía subsidiaria y luego trabajó para Sony en el año 2000 hasta el 2002. En el caso se hace mención de que este problema no solo lo tuvieron ellos dos, sino que también miles de empleados de la compañía. También hace mención de que Brian Krebs, investigador de seguridad, que pudo ver archivos de miles de empleados de Sony. A esto se añade que cabe recalcar que para el año 2011 Sony no cumplía con los estándares de seguridad tras una violación de datos que años anteriores a que este caso salió a relucir. Todo este problema surge ya que la información de ambos de mandantes estaba comprometida de cierta forma, es decir, la información de ambos demandantes y en nombre de todas las personas que fueron afectadas por este problema, su información personal, médica, entre otra información delicada, fue expuesta a medios públicos donde cualquier persona tenía acceso a ello.

Cabe recalcar que, para los estudios de este caso, no se hace mención de alguna demanda directa o indirecta al grupo de piratas informáticos o “GOP”. A su vez la demanda fue una directa a la compañía Sony Pictures Entertainment, Inc.

**La Gran Brecha de Sony 2000**

La compañía ha sufrido varios problemas en lo que respecta a la seguridad de sus sistemas. El caso de Michael Corona y Christina Mathis no ha sido la primera vez que sus sistemas no han trabajado de la forma que supone que trabajen. Sin embargo, Jasón Spaltro, el Director Ejecutivo de seguridad de la información de Sony, hizo una decisión comercial en noviembre de 2005 para no garantizar la seguridad de la red de Sony, según lo informado por el sitio web de tecnología y negocios CIO (Hornyak, 2014). En ese momento, ya se le encontraban fallas al sistema de seguridad, luego de haberse realizado una inspección por un auditor que completó una revisión de los mismos, ya que esto es un requisito importante de Sarbanes-Oxley.

En el 2007, Spaltro expuso en una entrevista con el CIO (Hornyak, 2014) que no estaba dispuesto a invertir dinero para defender la información confidencial de Sony expresando que “es una decisión comercial válida aceptar el riesgo”. Para el mes de mayo de 2009, se encontraron informes de que copias no autorizadas de Sony de las tarjetas de crédito de los clientes fueron enviadas por correo electrónico a una cuenta externa.

Pare enero de 2011, los piratas informáticos pudieron acceder al sistema de Sony, haciendo que el juego de PlayStation Modern Warfare 2 fuera imposible de jugar a través de PlayStation Network. Ya para abril de 2011, los piratas informáticos, habían robado millones de cuentas de usuario del servicio de juegos en línea. En ese entonces Sony recibió varias amenazas directas por parte de Anonymus como se menciona en el caso) de ataque de redes, pero Sony no implementó ningún tipo de protección. Según Engadget.com (2011), el director de información de Sony Corporation, Shinji Hasejima, admitió en una conferencia de prensa que la red de Sony no estaba segura en el momento de la violación de datos de abril de 2011 y afirmó que el ataque era una “vulnerabilidad conocida” (ya desde entonces podemos ver la Negligencia por parte de Sony en aspectos de seguridad para el caso). Para junio de 2011, el vicepresidente de Sony, según los informes, admitió que la red de Sony no cumplió con los estándares mínimos de seguridad en el momento de la violación de datos de abril de 2011.

En respuesta a la violación de datos de abril de 2011, Sony implementó medidas básicas para defenderse de nuevos ataques, incluidos los siguientes sistemas que deberían haberse implementado antes de abril de 2011: monitoreo automatizado de software; cifrado de datos mejorado; capacidad mejorada para detectar intrusiones en la red, como un sistema de alerta temprana para detectar patrones de actividad inusuales; y firewalls adicionales. La fuente de información Business Week citada por Warner (2014), informó que la causa de la violación de abril de 2011 fue que Sony perdió el control de sus claves criptográficas, −que también es el foco de varias firmas de seguridad que investigan el presente incumplimiento de datos de la red de Sony− y señaló que, si Sony nuevamente perdió el control de sus claves criptográficas, plantea la pregunta de por qué no las había protegido más de cerca tres años después. La demanda colectiva en nombre de los jugadores siguió en abril de 2011 por incumplimiento y Sony acordó liquidar esas reclamaciones en junio de 2014 a cambio de $15 millones en juegos, moneda en línea y reembolso por robo de identidad. Aun así, la falla de Sony para evitar incumplimientos de datos continuó después de abril de 2011.

Para mediados del 2014, los piratas informáticos volvieron a destruir el sistema de PlayStation Network, haciendo ataques cibernéticos a Sony; esto luego de que Sony resolviera el litigio de la demanda colectiva del 2011. En diciembre de 2014, la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés) lanzó una investigación sobre la intrusión cibernética de Sony y ofreció asesoramiento a los empleados sobre cómo gestionar la filtración de su información personal en el masivo incumplimiento de Sony Network Data.

**Descripción de hechos**

Basado en lo expuesto en el caso, los demandantes Michael Corona vs. Christina Mathis (Court Listener, 2014; Leagle, 2015), crean una demanda sobre la famosa compañía Sony Pictures Entertainment, Inc. Ambos demandantes fueron empleados para la compañía antes mencionada. Los mismos alegan que su información personal, médica, entre otra información sensitiva fue expuesta al público por un ataque cibernético a la compañía. Sony Pictures, fue “hackeada” por un grupo de hackers que se hacen llamar “Guardianes de la Paz” (mejor conocidos como “GOP”). Este grupo de hackers se encargó de exponer, no tan solo la información de los demandantes, sino que también expusieron información de una cantidad inmensa de empleados actuales de la compañía, contraseñas de la compañía y también expusieron una cantidad de correos electrónicos relacionados a los ejecutivos de la compañía.

También exponen en el caso que la compañía ya había sido advertida sobre la falla en el sistema por el equipo de auditores de la misma compañía. Como bien menciona en el caso por la parte del demandante Michael Corona, siendo este un ex empleado y desde el 2007 no trabaja para la compañía, no solo fue expuesta la información de él, sino que también se expuso la información de su esposa e hija. Corona tuvo que invertir sobre $700 dólares para un plan de protección para él y su familia. Por otra parte, Christina Mathis, esta fue empleada por una compañía que trabajaba para Sony y también fue empleada desde 2000 hasta el 2002, tuvo la misma situación que Corona. Esta tuvo que invertir en un plan de protección y otras diligencias relacionadas al caso por un monto de sobre $300 dólares anuales solo para lo relacionado al caso. Después de los hechos los demandantes le piden al tribunal la oportunidad de que otros se puedan a unir a esta demanda haciendo de esta una colectiva en conformidad con la Regla 23 de la Reglas Federales, según expuesta en el caso. Además de exponer que esto se trataría de una demanda millonaria, también piden una serie de condiciones a lo que el caso es investigado. Alguno de estos alivios mencionados en el caso son:

1. Que el Tribunal certifique este caso como una demanda colectiva de conformidad con la Regla de Procedimiento Civil 23 (a), (b) (2) y (b) (3), y, de conformidad con la Regla Federal de Procedimiento Civil 23 (g), designe a los Demandantes y los abogados defensores de los Demandantes representar dicha Clase;
2. Descubriendo que Sony incumplió su deber de salvaguardar y proteger la información personal de los Demandantes y la Clase que se vio comprometida en la violación de seguridad que se convirtió en conocimiento público a partir de noviembre de 2014;
3. Que el Tribunal adjudique a los Demandantes y al desagravio apropiado de la Clase, incluyendo cualquier daño real y legal, restitución y devolución.
4. Que la Corte otorgue una medida equitativa, cautelar y declarativa como puede ser apropiado según las leyes estatales aplicables. Los Demandantes, en nombre de la Clase, buscan medidas cautelares apropiadas, que incluyen, entre otras: (i) la provisión de servicios de monitoreo de crédito y/o supervisión de tarjetas de crédito para la Clase durante al menos cinco años; (ii) la prestación de servicios de supervisión bancaria y/o supervisión bancaria para la Clase durante al menos cinco años; (iii) la provisión de un seguro de robo de identidad para la Clase durante al menos cinco años; (iv) la provisión de servicios de restauración de crédito para la Clase durante al menos cinco años; (v) adjudicar a los Demandantes y la Clase los costos y gastos razonables de la demanda, incluidos los honorarios de los abogados, los honorarios de presentación y el seguro de la Clase; y (vi) exigir que Sony reciba auditorías periódicas de cumplimiento por parte de un tercero sobre la seguridad de sus sistemas informáticos utilizados para almacenar datos de empleados actuales y anteriores, para evitar la recurrencia de una violación de datos mediante la adopción e implementación de mejores prácticas de datos de seguridad;
5. Adjudicación de los daños solicitados en este documento a los Demandantes y la Clase;
6. Adjudicación de todos los costos, incluidos los honorarios de los expertos y los honorarios de los abogados, y los costos de enjuiciar esta acción;
7. Adjudicación de intereses previos y posteriores al juicio según lo prescrito por ley;
8. Conceder alivio legal o equitativo adicional.

**Acusaciones, cargos y términos**

**Negligencia**

Se le imputa este cargo ya que la compañía Sony Pictures Entertainment, Inc., faltó al incumplir con su deber de proteger y salvaguardar la información personal de los demandantes y sus empleados. Por sus comportamientos y acciones, Sony incumplió ya que los mismos tenían conocimiento de lo que estaba aconteciendo y esto no llevaron la comunicación correcta o se comunicaron debidamente con sus empleados o personas que estuvieran involucradas directa o indirectamente, haciendo que los mismos incurrieran en gastos para poder proteger y lidiar con el problema de cuidar y poder proteger todo lo relacionado a información personal.

**Violación de la confidencialidad de California de Ley de Información Médica, Cal. Civ. Código § 56, et seq.**

Este cargo es imputado ya que el mismo prohíbe a los empleadores a divulgar información médica sin consentimiento previo del paciente. En el curso normal, los empleadores pueden poseer parte de un registro médico de sus empleados, de esta forma se encuentra la falta por parte de Sony ya que el mismo no garantizó la existencia de sistemas de seguridad adecuado o impedir el acceso y la divulgación de la información médica privada de los demandantes, violando así la Ley de Información Médica y su obligación legal de proteger la confidencialidad de dicha información.

**Violación del Código Civil de California, Cal. Civ. Código § 1798.80 et seq.**

**(En nombre del demandante Mathis y la subclase de California)**

Acusación por Incumplimiento de la notificación de información personal.

Podemos explicar esto como apropiación ilegal de información por parte de la compañía Sony ya que esta violación al Cal. Civ. Código § 1798.80 et seq. lo que nos explica es que una persona o empresa que realiza negocios en California, y que posee o licencia datos informatizados que pueden incluir información personal, debe revelar una violación de la seguridad del sistema después del descubrimiento o notificación de la violación en la seguridad de los datos a un residente de California. Con esto expuesto según el código podemos ver la falla de Sony al no tener la comunicación correcta con su personal al saber por la situación que podían atravesar las personas a las cuales su información personal privada (PII) había sido expuesta.

**Violación del Código Civil de Virginia § 18.2-186.6., Et seq. (Código de Virgina)**

**(En nombre del demandante Corona y la subclase de Virginia)**

Acusación por incumplimiento de la notificación de información personal.

Según es expuesto en el caso y en el Código Civil de Virginia.

A lo que se refiere a violación de seguridad de sistemas se refiere al acceso no autorizado y el beneficio de los datos computarizados no encriptados y no modificados que comprometen la seguridad, privacidad o confidencialidad de la PII de los demandantes y la clase por un individuo o entidad. Por otra parte, también se hace mención de los datos encriptados que se hace definir con la transformación de datos mediante el uso de un progreso algorítmico con una baja probabilidad de que tenga un uso de proceso o clave. También hace mención del incumplimiento por falta de comunicación efectiva y notificación de parte del acusado para con el demandante en base a lo que el problema de robo de PII se refiere y la información que haya sido expuesta al público.

**Definición de términos**

1. Robo de Identidad – esto se basa cuando a una persona es víctima de robo de información personal como, por ejemplo: número de Seguro Social, dirección entre otras cosas. Mayormente esto sucede para luego cometer un fraude utilizando la información robada.
2. Fraude – además de ser un delito mayormente realizado para obtener un poder económico o político, es una forma de corrupción, utilizando el engaño o la mentira para así obtener el beneficio deseado.
3. Ataque − es la forma en que se realiza efectivamente una amenaza intencionalmente.
4. Seguridad de computadoras y/o de redes de información – es más bien todo aquello que se encarga de la protección de los datos o las informaciones en un sistema o red. Evitando destrucción de información, modificación de la información, robo, remoción o pérdida de la información o los recursos. También existe la seguridad del hardware y del software.
5. Criptografía – es mejor conocido como el arte de escribir claves ocultas. Es más bien un conjunto de técnicas para lograr protege u ocultar alguna información bajo un código. Existen varias clases como la híbrida, la asimétrica y la simétrica.
6. Numerosidad − a lo que el caso se refiere; se refiere a la cantidad extensa de empleados y ex empleados de la compañía que su PII fue comprometida.
7. Tipicidad – a lo que el caso se refiere; es o típico de los reclamos y alegaciones de los demandantes y la clase ante el ataque y la vulnerabilidad de los sistemas de la compañía Sony.
8. Adecuación − a lo que el caso se refiere; es más bien la adaptación de los demandantes y la aceptación o el comportamiento de estos hacia el acusado y las diferentes situaciones que enfrenten por el problema.
9. Superioridad − a lo que el caso se refiere; es el conjunto de la clase junto a los demandantes y de esta forma no se cree una inconsistencia de parte delo los demandantes principales ya que los mismos intentan tener una demanda colectiva.
10. PII − Mejor conocido por sus siglas en inglés “personal identifying information” o identificación de información personal, es cualquier información sensible o no sensible que se pueda utilizar para la identificación de una persona.
11. Violación de la seguridad del sistema − significa el acceso sin autorización y la adquisición de datos computarizados no editados y sin cifrar que comprometen la seguridad o confidencialidad de la información personal. En este caso se refieren la información de los demandantes y de la clase.
12. Clase − Grupo de personas no mencionadas en el caso, pero directamente afectadas de la misma forma que los demandantes principales.
13. Piratas informáticos − A lo que el caso se refiere; corresponde a los llamados “Hackers” o piratas cibernéticos, es decir, el grupo de personas que se encarga o se dedica al robo de información o la piratería.

**SECCIÓN 2: REVISIÓN DE LITERATURA**

**Introducción**

El fraude cibernético se refiere al fraude que es realizado a través del uso de una computadora o el internet. Este fraude o delito informático puede ser realizado como, por ejemplo, a través de correos electrónicos, mensajes de texto, mensajería instantánea, medios sociales y a través de otras fuentes que estén relacionadas a algún sistema de información y que este tenga fallas en sus sistemas de seguridad. En los Estados Unidos existe una entidad u organización que realiza un estudio anual sobre la Seguridad Informática y los crímenes cometidos a través de las computadoras. Computer Security Investigation (2000) realizó un estudio donde 273 [instituciones](http://www.monografias.com/trabajos13/trainsti/trainsti.shtml), grandes Corporaciones y Agencias del Gobierno fueron parte de una investigación donde el enfoque era el estudio de seguridad y delitos informáticos. La investigación reflejó los siguientes resultados:

|  |
| --- |
| Respuestas |
| No reportaron violaciones de seguridad 10%  Reportan Violaciones de Seguridad 90% |
| http://www.monografias.com/trabajos6/delin/Image1433.gif |
|  |

*Figura 1.*  Estadística de reportes de violaciones a la seguridad informática

*Figura 1.* Andrés, J. (2014). *Estadísticas sobre los delitos informáticos*. Recuperado de, http://legislacionunicesar2014.blogspot.com/2014/06/estadisticas-sobre-los-delitos.html

En el reporte mostrado anteriormente podemos observar que el 90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses. De otra parte Recovery Labs Division Computer Forensic (2015), establece que existen distintos tipos de fraudes cibernéticos, estos son:

1. **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:**
2. Acceso ilícito a sistemas informáticos.
3. Interceptación ilícita de datos informáticos.
4. Interferencia en el funcionamiento de un sistema informático.
5. Abuso de dispositivos que faciliten la comisión de delitos.
6. Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.
7. **Delitos informáticos:**
   1. Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
   2. Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos. El borrado fraudulento de datos o la corrupción de ficheros son algunos ejemplos de delitos de este tipo.
8. **Delitos relacionados con el contenido:**
   1. Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.
9. **Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:**
   1. Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

**Leyes Aplicables**

De acuerdo con la documentación del caso de Michael Corona & Christina Mathis vs. Sony Pictures Entertainment Inc. Se le acusa a Sony de:

**Negligencia**

Se le acusa por este cargo a Sony Pictures Entertainment Inc. ya que según es estipulado en el caso Sony tenía una obligación con los Demandantes y los miembros de la Clase de proporcionar seguridad, incluso conforme a los estándares y requisitos de la industria, para garantizar que sus sistemas y redes, y el personal responsable de ellos, protejan adecuadamente la PII de sus empleados actuales y anteriores.

**Violación de la confidencialidad de California de Ley de Información Médica, Cal. Civ. Código § 56, et seq.**

Según el código Civil de California § 56, et seq., conocido como la Ley de Confidencialidad de Información Médica ("Ley de información médica") exige a los empleadores que reciben información médica que establezcan los procedimientos adecuados para garantizar la confidencialidad y protección contra el uso no autorizado y la divulgación de esa información. Estos procedimientos pueden incluir, pero no están limitados a, instrucción con respecto a la confidencialidad de los empleados y agentes que manejan archivos que contienen información médica y sistemas de seguridad que restringen el acceso a archivos que contienen información médica.

**Violación de Cal. Civ. Código § 1798.80 et seq.**

**(En nombre del demandante Mathis y la subclase de California)**

Según es expuesto en el caso y la sección 1798.82 del Código Civil de California establece, en lo pertinente, parte de la siguiente manera:

(b) Cualquier persona o empresa que mantiene datos computarizados que incluye información personal que la persona o empresa no propio deberá notificar al propietario o licenciatario de la información de cualquier violación de la seguridad de los datos inmediatamente después del descubrimiento, si la información personal era, o se cree razonablemente que lo ha sido, adquirido por una persona no autorizada.

(d) Cualquier persona o empresa que está obligada a emitir una violación de seguridad notificación de conformidad con esta sección deberá cumplir con todos los siguientes requisitos:

(1) La notificación de violación de seguridad se escribirá sin idioma.

(2) La notificación de violación de seguridad deberá incluir, a mínimo, la siguiente información:

(A) El nombre y la información de contacto de los informes persona o empresa sujeta a esta sección.

(B) Una lista de los tipos de información personal que fueron o se cree razonablemente que han sido objeto de un incumplimiento.

(C) Si la información es posible de determinar en el momento la notificación se proporciona, a continuación, cualquiera de los siguientes: (i) la fecha de la infracción, (ii) la fecha estimada de la infracción, o (iii) el rango de fechas dentro del cual ocurrió la violación. La notificación también incluirá la fecha del aviso.

(D) Si la notificación se retrasó como resultado de una ley e investigación de ejecución, si esa información es posible para determinar en el momento en que se proporciona el aviso.

(E) Una descripción general del incidente de infracción, si eso es posible determinar la información en el momento que la notificación está provisto.

(F) Los números de teléfono gratuitos y las direcciones de principales de agencias de informes de crédito si la violación expuesta a número de seguro social o una licencia de conducir o Número de Tarjeta de Identificación de California.

(f) Cualquier persona o empresa que esté obligada a emitir una violación de seguridad notificación de conformidad con esta sección a más de 500 residentes de California como consecuencia de una infracción única del sistema de seguridad debe enviar electrónicamente una copia que muestra una notificación, excluyendo cualquier información de identificación personal, a la Fiscal General. Una copia de muestra única de una violación de seguridad notificación no se considerará dentro de la subdivisión (f) de Sección 6254 del Código de Gobierno.

(g) Para los propósitos de esta sección, “violación de la seguridad del sistema” significa la adquisición no autorizada de datos computarizados que compromete la seguridad, la confidencialidad o la integridad de la información personal mantenida por la persona o empresa. Buena fe adquisición de información personal por un empleado o agente de la persona o empresa para los fines de la persona o empresa no es una violación de la seguridad del sistema, siempre que la información no se usa o está sujeta a una divulgación no autorizada adicional.

1. La adquisición no autorizada de PII de los Demandantes y los Miembros de la Clase constituyó una "violación del sistema de seguridad" de Sony.
2. Sony retrasó irrazonablemente informar a alguien sobre el incumplimiento de la seguridad de la información confidencial y no pública de los miembros de subclase de California después de que Sony supiera que se había producido una violación de datos.
3. El demandado no divulgó a los miembros de la subclase de California, sin retraso irrazonable, y en el tiempo más conveniente posible, la violación de la seguridad de su información personal identificable no encriptada o cifrada de forma segura cuando sabían o creían razonablemente que dicha información se había visto comprometida.
4. Ante la información y las creencias, ninguna agencia de orden público instruyó Sony, la notificación a los miembros de la Subclase de California impediría la investigación.
5. De conformidad con la Sección 1798.84 del Código Civil de California:

(a) Cualquier renuncia a una disposición de este título es contraria a la política pública y es nulo e inaplicable.

(e) Cualquier negocio que viole, proponga violar o haya violado este título puede ser ordenado.

1. Como resultado de la violación de Sony de Cal. Civ. Código § 1798.82, Californiana de esa violación de seguridad. Los miembros de la subclase incurrieron en daños económicos relacionados con los gastos del monitoreo de crédito y otros servicios de prevención de robo de identidad.
2. La Demandante Mathis, individualmente y en nombre de los miembros de la subclase de California, busque todos los remedios disponibles bajo Cal. Civ. Código § 1798.84, que incluye, pero no se limita a: (a) los daños sufridos por los miembros de la Subclase de California como se alega anteriormente; y (b) alivio equitativo.

**Violación de § 18.2-186.6., Et seq.**

**(En nombre del demandante Corona y la subclase de Virginia)**

Por otra parte, **s**egún es explicado en el caso la “Violación de la seguridad del sistema” significa el acceso no autorizado y la adquisición de datos computarizados no editados y sin cifrar que compromete la seguridad o confidencialidad de la información personal mantenida por un individuo o entidad como parte de una base de datos de información personal con respecto a múltiples individuos y que causa, o la persona o entidad cree razonablemente que ha causado, o causará, robo de identidad u otro fraude a cualquier residente de la Commonwealth. La adquisición no autorizada de PII de los demandantes y los miembros de la demanda colectiva constituido una "violación de la seguridad del sistema" de Sony bajo la Sección 18.2- 186.6.A. del Código de Virginia.

**Casos Relacionados**

**Robo de información a la compañía Target Corporation**

Abrahams (2017) nos presenta un breve resumen de los ocurrido el pasado diciembre de 2013, donde la compañía Target Corporation sufrió un robo de información de sobre 40 millones de clientes. La misma fue expuesta al público por los hackers que crearon el ataque. En el ataque se filtraron números de tarjetas de crédito, información personal de los clientes, emails y direcciones residenciales. El ataque se produjo en una de las mismas tiendas por departamentos de Target por parte de los hackers, llevando a la compañía a tener que pagar alrededor de $18.5 millones de dólares a 47 diferentes estados incluyendo al distrito de Columbia como parte del acuerpo por los abogados del estado para cubrir la falla de seguridad que comprometió los datos de millones de clientes.

De acuerdo con Waterstehnology (2015) en febrero 2015 hackers realizaron el mayor ataque cibernético a instituciones financieras alrededor del mundo, realizando una brecha en sistema de seguridad que consistió en no solo robar información, sino que robaron millones de dólares. Esta brecha fue notada primeramente por Kiev, Ukrania cuando las ATM comenzaron a distribuir dinero sin ningún tipo de interacción humana. La compañía especializada en seguridad cibernética Kaspersky Labs investigó y encontró que un grupo de hackers rusos operando bajo el seudónimo de “Carabank” utilizaron un malware escondido en cuentas de correo electrónico en el sistema bancario en el cual registraron acciones de los cajeros del personal de banco al pulsar las teclas y utilizaron esta información para transferir dinero en cuentas fraudulentas. Se estimó en cerca de un billón de dólares el total que saquearon los hackers.

Estos son algunos de los ataques cibernéticos reportados recientemente. En la próxima sección se recrea el proceso realizado por los hackers en el ataque cibernético a Sony Entertainment Inc.

**SECCIÓN 3: SIMULACIÓN**

En esta sección se presenta la simulación de proceso que siguieron los hackers para entrar al sistema de Sony Entertainment Inc. y violar la seguridad del mismo. Se presentan en figuras el proceso en que ocurrió el ataque cibernético.

En la Figura 2, podemos observar cómo el atacante logra obtener accesos al Sistema utilizando una cuenta de administrador.

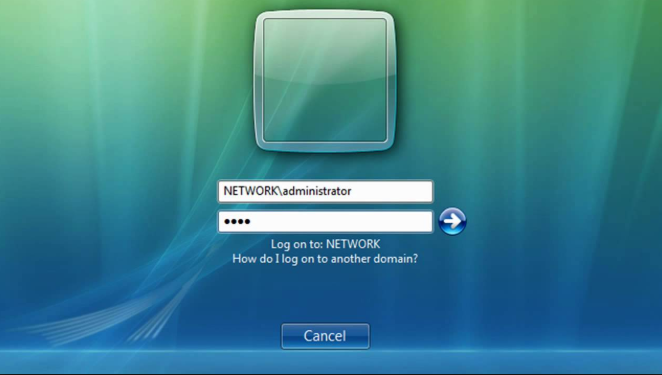


Figura 2. Acceso al sistema, Cuenta administradora

En la Figura 3, podemos observar cómo una vez dentro de la computadora de la compañía el atacante conectó su memoria externa para trasferir el archivo que contenía el malware.

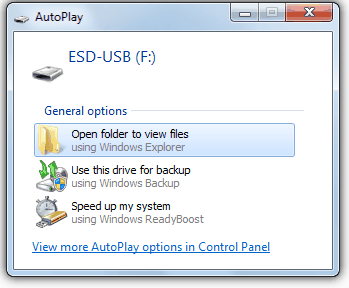


Figura 3. Primera conexión de los hackers e instalación de archivos para atacar el sistema.

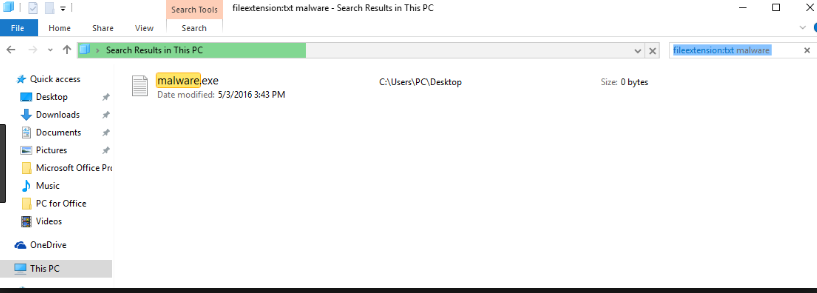
En la Figura 4, podemos observar el malware que se encontraba en la memoria externa y el cual el hacker ejecutó en la computadora que obtuvo acceso.

Figura 4: Instalación del malware al sistema

En la Figura 5, podemos observar cómo una vez el malware fue ejecutado las computadoras de la compañía comenzaron a presentar la siguiente pantalla en el momento que los empleados de la compañía intentaban entrar al sistema.



Figura 5. Aviso por parte de los hackers luego de instalar el malware en el sistema.

*Figura 5*. Schroeder, S. (2014). *Massive hack takes down Sony Pictures' computer system*. Recuperado de, <https://mashable.com/2014/11/25/hack-sony-pictures/#v0j1HXbC.Pqw>

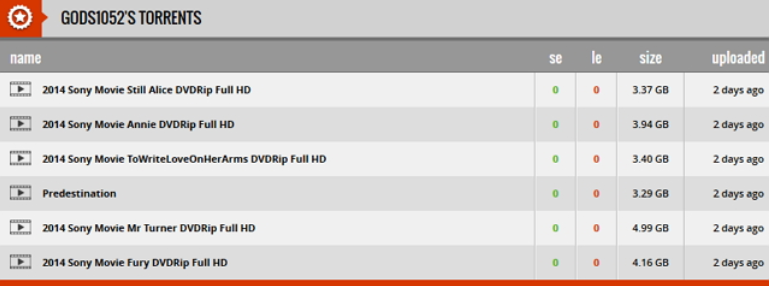
En la Figura 6 se puede observar la primera ronda de archivos que fueron difundidos en la Internet por el grupo de hackers. Donde presentan varias películas que aún no estaban disponibles.

Figura 6. Primera exposición de archivos (películas) al público por parte de los hackers

*Figura 6.* Andy. (2014). *Sony movies leak online after hack attack.* Recuperado de, https://torrentfreak.com/sony-movies-leak-online-after-hack-attack-141129/

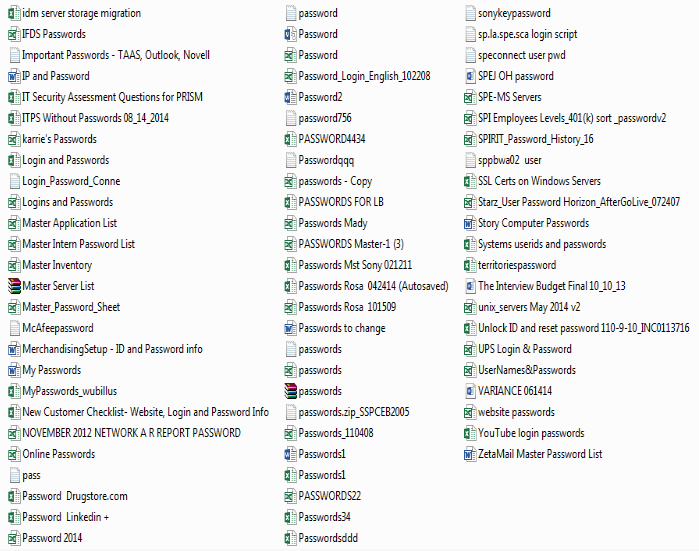
En la Figura 7 se muestran archivos que contenían información de contraseñas que la compañía utilizaba, las mismas siendo expuestas al público.

Figura 7. Contraseñas de empleados expuestas al público.

*Figura 7.* RiskBased Security. (2014). *A breakdown and analysis of the December, 2014 Sony hack*. Recuperado de, <https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/>

En la Figura 8, podemos observar 22 archivos en formato “torrent” los cuales

contenían información financiera de la compañía.

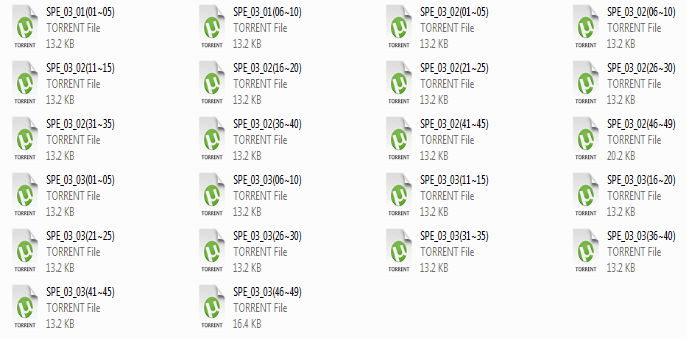


Figura 8. Exposición de los documentos financieros de la compañía y empleados.

*Figura 8*. RiskBased Security. (2014). A breakdown and analysis of the December, 2014 Sony hack. Recuperado de, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

En la Figura 9, se presenta un segundo mensaje de parte del grupo de hackers el cual fue divulgado en la página “Pastbin” por el grupo de hackers.

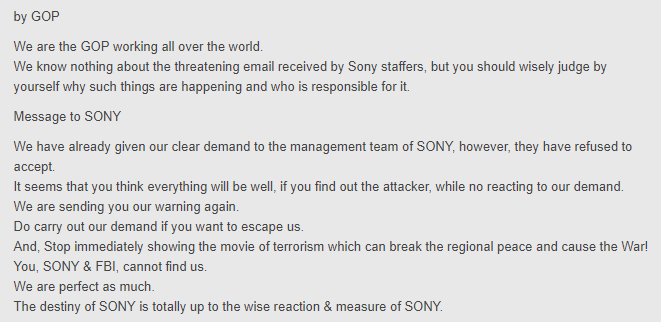
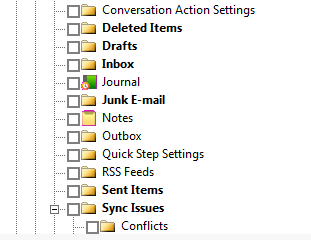
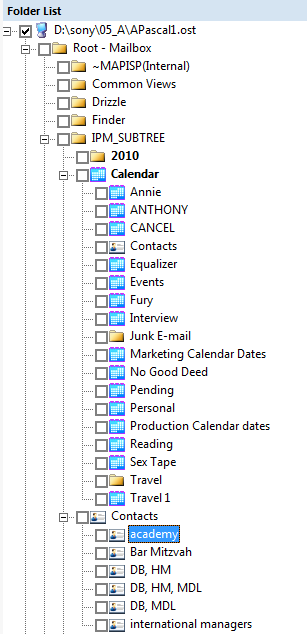


Figura 9. Segundo comunicado de los hackers utilizando la página “Pastbin”

*Figura 9*. RiskBased Security. (2014). A breakdown and analysis of the December, 2014 Sony hack. Recuperado de, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

En la figura 10, podemos observar la cuenta de Outlook de Amy Pascal, Co-Director de Sony en el momento de los ataques.



*Figura 10. Cuenta de Outlook de Amy Pascal, Co Director de Sony en el ataque*

*Figura 10*. RiskBased Security. (2014). A breakdown and analysis of the December, 2014 Sony hack. Recuperado de, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

En la Figura 11, se presenta el texto de un email que fue enviado a varios directores de la compañía y el cual se pudo obtener de la cuenta de email de Amy Pascal.

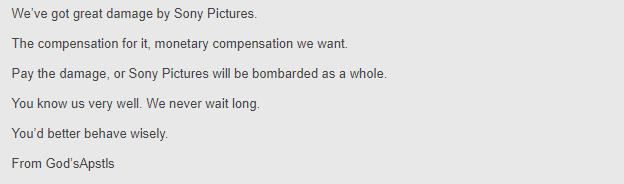


Figura 11. Ccomunicado de los hackers a través del email de Amy Pascal.

*Figura 11*. RiskBased Security. (2014). A breakdown and analysis of the December, 2014 Sony hack. Recuperado de, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

En la Figura 12, podemos observar otra declaración por parte del grupo de hackers “GOP” la cual se encontraba dentro del archivo divulgado.

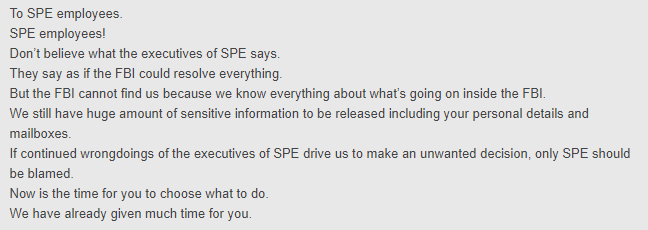


Figura 12. Comunicado por parte de GOP en el sistema.

*Figura 12*. RiskBased Security. (2014). A breakdown and analysis of the December, 2014 Sony hack. Recuperado de, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

En la Figura 13, se presenta otro archivo que fue expuesto a la luz pública el cual contenía información de otras compañías que en algún momento o actualmente se relacionaban con Sony.

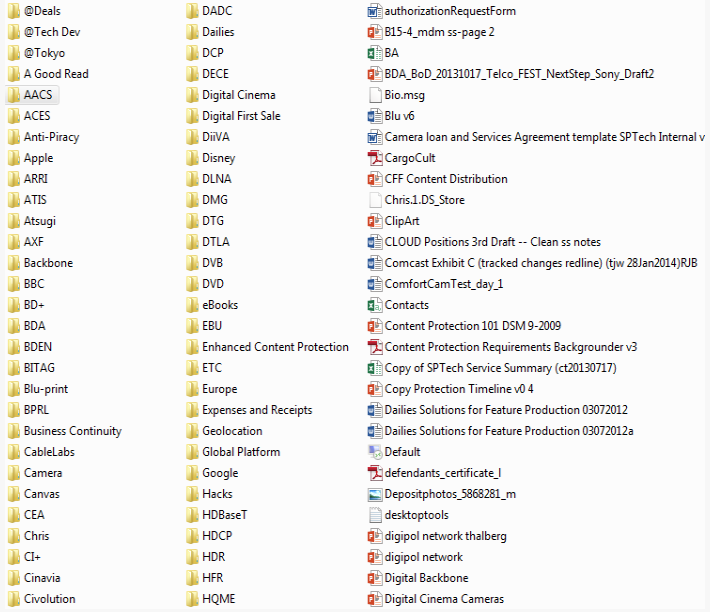


Figura 13. Archivos difundidos por los hackers.

*Figura 13*. RiskBased Security. (2014). A breakdown and analysis of the December, 2014 Sony hack. Recuperado de, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

En la figura 14, podemos observar un tercer comunicado el cual fue creado en la página de “Pastebin”.

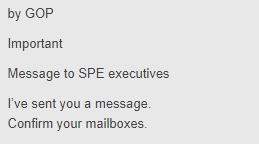
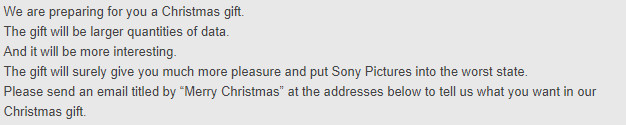


Figura 14. Comunicado de los hacker por la página “Pastebin”

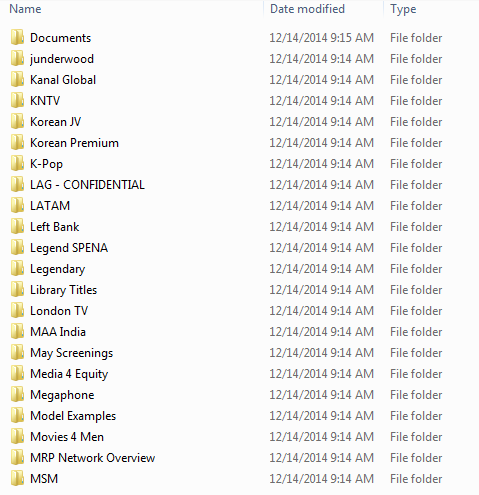
*Figura 14*. RiskBased Security. (2014). A breakdown and analysis of the December, 2014 Sony hack. Recuperado de, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

En la Figura 15, se exhibe otro mensaje que acompaño al comunicado que presentamos en la figura anterior.

 Figura 15: Comunicado por los hackers

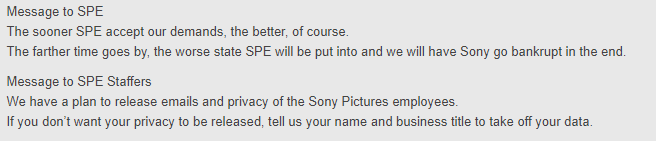
*Figura 15*. RiskBased Security. (2014). A breakdown and analysis of the December, 2014 Sony hack. Recuperado de, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

En la Figura 16, podemos prestar atención a los archivos que fueron divulgados al mismo tiempo que enviaron su tercer comunicado.

 Figura 16: Lista de archivos expuestos

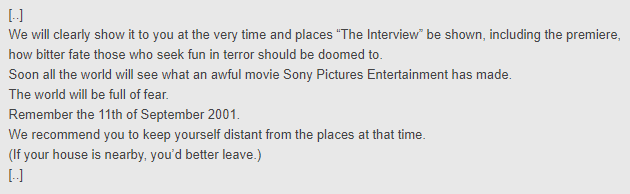
*Figura 16*. RiskBased Security. (2014). A breakdown and analysis of the December, 2014 Sony hack. Recuperado de, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

En la Figura 17, se presenta el cuarto comunicado por parte del grupo de hackers “GOP”.

 Figura 17. Comunicado de los hackers en el sistema

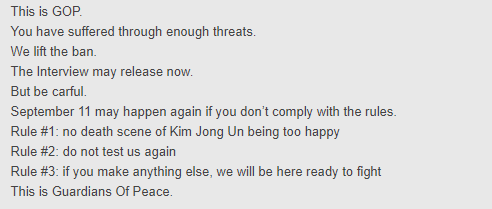
*Figura 17*. RiskBased Security. (2014). A breakdown and analysis of the December, 2014 Sony hack. Recuperado de, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

En la Figura 18, podemos observar el quinto comunicado de parte de los atacantes.

 Figura 18. Comunicado del GOP a través del sistema de la compañía

*Figura 18*. RiskBased Security. (2014). A breakdown and analysis of the December, 2014 Sony hack. Recuperado de, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

En la Figura 19, podemos observar el sexto y último comunicado del grupo “GOP” a Sony Entertainment Inc.

 Figura 19. Último comunicado de GOP

*Figura 19*. RiskBased Security. (2014). A breakdown and analysis of the December, 2014 Sony hack. Recuperado de, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

**SECCIÓN 4: INFORME DEL CASO**

**Resumen Ejecutivo**

La empresa Sony Pictures Entertainment Inc., es una distribuidora y productora estadounidense de cine, su dueño es Sony Corporation un conglomerado de tecnología multinacional y medios de comunicación con sede en Japón. Los demandantes Michael Corona y Christina Mathis han solicitado los servicios de Josué Rivera investigador digital forense para analizar la cantidad de data personal de los demandantes que fue divulgada públicamente. El fiscal Gary Klausner, del Distrito Central de California, entrega al investigador Josué Rivera un dispositivo de almacenamiento el cual contenía los archivos que fueron difundidos y contenían información personal de empleados tanto activos como retirados de la compañía. Para analizar la data se utilizará la herramienta digital Forensic Tool Kit (FTK). Este software brindará la oportunidad de trabajar la data de una manera diferente. De igual manera permite escanear el dispositivo de almacenamiento en búsqueda de información relacionada al caso. Al culminar el análisis, se detectó un archivo dentro del dispositivo de almacenamiento que contenía un sinnúmero de documentos de empleados de Sony incluyendo información de los demandantes.

**Objetivo**

Es de suma importancia analizar el sistema de almacenamiento de manera profunda para descubrir el mayor número de data que se relacione con los demandantes para así lograr lazar la falta y el daño ocasionado a los demandantes. Los demandantes Michael Corona y Cristina Mathis contrataron los servicios de Josué Rivera con el objetivo de estudiar y/o analizar, encontrar y recuperar información sensitiva filtrada mediante los hackers por diferentes plataformas con el propósito de recuperar la información personal de los demandantes.

**Alcance del trabajo**

Josué O. Rivera, Empleado de la compañía IT Tech Solutions, tiene la encomienda de analizar, recuperar y proteger todo tipo de información que sea relativa al caso. Los resultados de este análisis servirán de ayuda en el caso ya que confirmarán el vínculo directo de Sony con la data filtrada de los demandantes. El sistema de almacenamiento y su contenido será analizado de una manera profunda lo cual permitirá descubrir la mayor cantidad de data. La data que se encuentra en el USB fue recolectada por el demandante. El USB será identificado como A-1-2014-1. Durante el proceso de análisis se utilizará la herramienta de investigación digital FTK.

**Datos del caso**

Número del Caso: 2:14-cv-09600-RGK-E

Examinador: Josué O. Rivera Morales

Investigador del Caso: John Hallmark del Distrito de California.

**Descripción de los dispositivos utilizados**

Los dispositivos utilizados durante el proceso lo fueron:

1. Laptop HP modelo BS087, computadora que contiene las aplicaciones necesarias para el análisis de la data.
2. USB Western Digital Modelo 32 GB. El mismo guarda todos los documentos que el demandante pudo recolectar referentes al caso.

Las herramientas de investigación son de gran importancia, ya que estas ayudan de gran manera a analizar y estudiar el ataque de una manera más organizada. De igual manera, brindan la oportunidad de entender cómo y porque el ataque se produjo. Algunas de las herramientas o programas que serán utilizadas en el análisis son:

1. Vuze - Es un programa P2P y un cliente de “Bittorrent” que permite el manejo de archivos torrents. Este programa facilita la descarga de distintos medios en los cuales los torrents son publicados (Azureus, 2018).
2. Google Chrome Browser - Es un navegador de red desarrollado por “Google” que se caracteriza por su interfaz sencillo, pero de mucha utilidad. De igual manera le permite al usuario navegar el internet de una manera rápida, sencilla y segura (Webopedia, 2018).
3. Forensic Toolkit (FTK) - Es una herramienta forense de computadora. Es reconocido como el software estándar. Dicha plataforma de investigación es validada por la corte internacional como la última tecnología de análisis forense de computadoras.

**Resumen de hallazgos**

Una vez el análisis fue culminado presentó un archivo dentro de la data en el USB que contenía todo tipo de información de información de empleados y exempleados como el demandante Christina Mathis. La data que contenía el archivo consistía de Seguro Social, fechas de nacimiento, salarios, información y récord médicos y un sin número de información.

**Cadena de custodia**

IT Tech Solution estableció una cadena de custodia desde el momento que el dispositivo de almacenamiento fue entregado. De igual manera la cadena de custodia fue establecida en el momento que se descubrió la evidencia. Manteniendo el proceso lo más íntegro posible para que la evidencia sea admisible en el tribunal. A continuación, podemos observar la cadena de custodia que IT Tech Solution siguió:

**Primer Evento**

1. Descripción del evento: El fiscal del Distrito de Central de California, hace entrega del dispositivo de almacenamiento el cual será analizado por IT Tech Solution.
2. Evento Verificado por: Josué O. Rivera y J. Hallmark
3. Número de Evidencia: A-1-2014-1
4. Fecha de comienzo: 12 de diciembre de 2014
5. Fecha de terminación: 14 de diciembre de 2014
6. Lugar de origen: Oficina del Fiscal;
7. Destino: Laboratorio Forense IT Tech Solution

**Segundo Evento**

1. Descripción del evento: Creación del número del caso y asignación de evidencia al mismo.
2. Evento verificado por: Josué O. Rivera
3. Número de evidencia: A-1-2014-1
4. Fecha de comienzo: 12 de diciembre de 2014
5. Fecha de Terminación: 14 de diciembre de 2014
6. Lugar de origen: Laboratorio Forense IT Tech Solution
7. Destino: Laboratorio Forense IT Tech Solution

**Tercero Evento**

1. Descripción del evento: Comenzar con el análisis de los documentos que se encuentran en el USB para presentar la evidencia recuperada en el reporte.
2. Evento verificado por: Josué O. Rivera
3. Numero de evidencia: A-1-2014-1
4. Fecha de comienzo: 12 de diciembre de 2014
5. Fecha de terminación: 14 de diciembre de 2014
6. Lugar de origen: Laboratorio Forense IT Tech Solution
7. Destino: Laboratorio Forense IT Tech Solution

**Cuarto Evento**

1. Descripción del evento: Se entrega el informe del análisis forense realizado al fiscal del caso.
2. Evento verificado por: Josué O. Rivera y J. Hallmark
3. Numero de evidencia: A-1-2014-1
4. Fecha de comienzo: 12 de diciembre de 2014
5. Fecha de terminación: 14 de diciembre de 2014
6. Lugar de origen: Laboratorio Forense IT Tech Solution
7. Destino: Oficina del Fiscal encargado del caso

**Quinto Evento**

1. Descripción del evento: Devolución de dispositivo de almacenamiento originalmente entregado por el Fiscal del Distrito a Josué O. Rivera investigador forense de IT Tech Solution Inc.
2. Evento verificado por: Josué O. Rivera y J. Hallmark
3. Número de evidencia: A-1-2014-1
4. Fecha de comienzo: 12 de diciembre de 2014.
5. Fecha de terminación: 15 de diciembre de 2014.
6. Lugar de origen: Laboratorio Forense IT Tech Solution
7. Destino: Oficinas legales de Sony Pictures Entertainment Inc.

**Procedimiento**

Cada proceso investigativo es trabajado de acuerdo a la seguridad y los protocolos establecidos por la compañía que representan. A continuación, se presentará el proceso de investigación que realizó Josué O. Rivera de la Compañía IT Tech Solution. Se estableció una cadena de custodia y se creó una copia del USB para así trabajarlo sin alterar la evidencia original. Abrimos Forensic Toolkit (FTK), en el cual se escoge la opción de crear una imagen nueva. El programa permite crear una imagen del dispositivo de almacenamiento, manteniendo así la data original intacta.

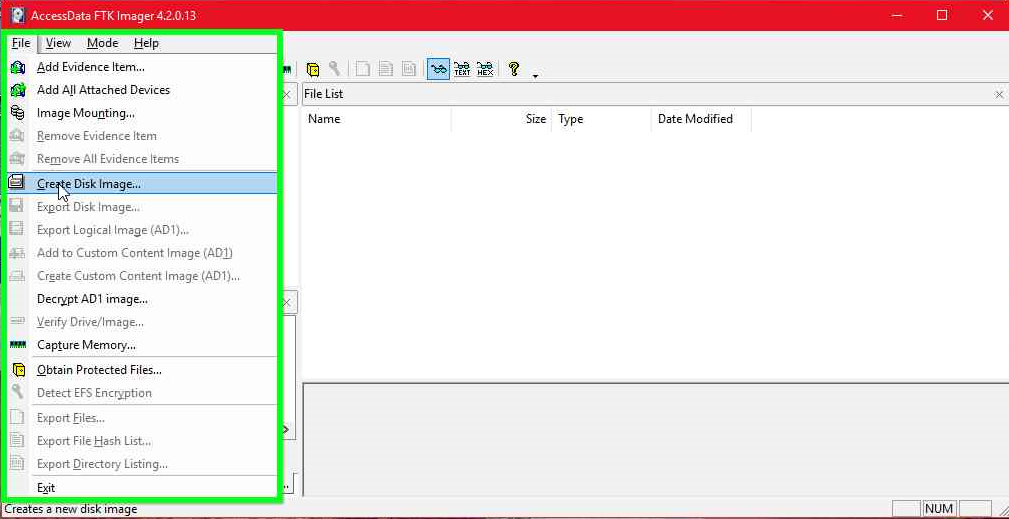
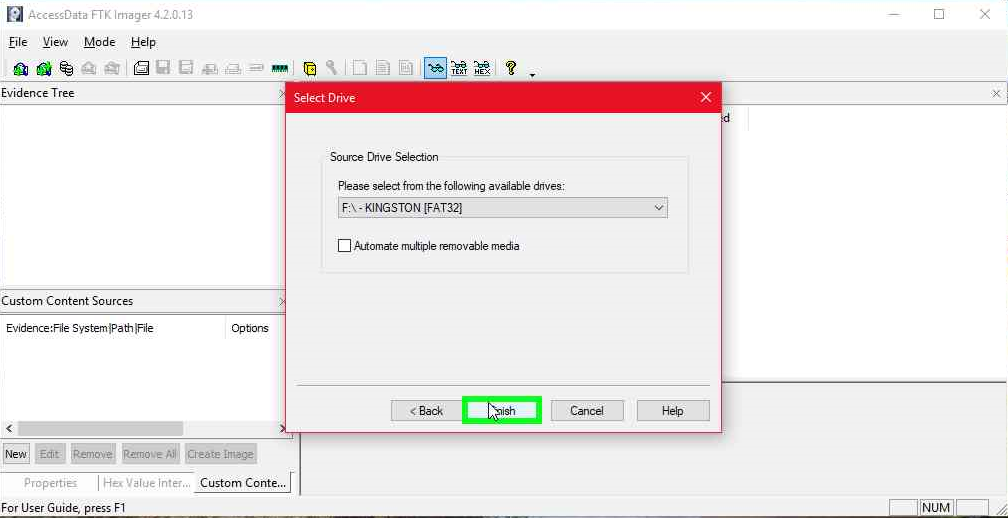


Figura 20. Página principal para el comienzo de análisis

Según se presenta en la Figura 21, se escoge la fuente de la evidencia que se encuentra en el USB.

 Figura 21. Fuente de evidencia en el USB

La Figura 22 presenta la entrada de información referente al caso que se está analizando.

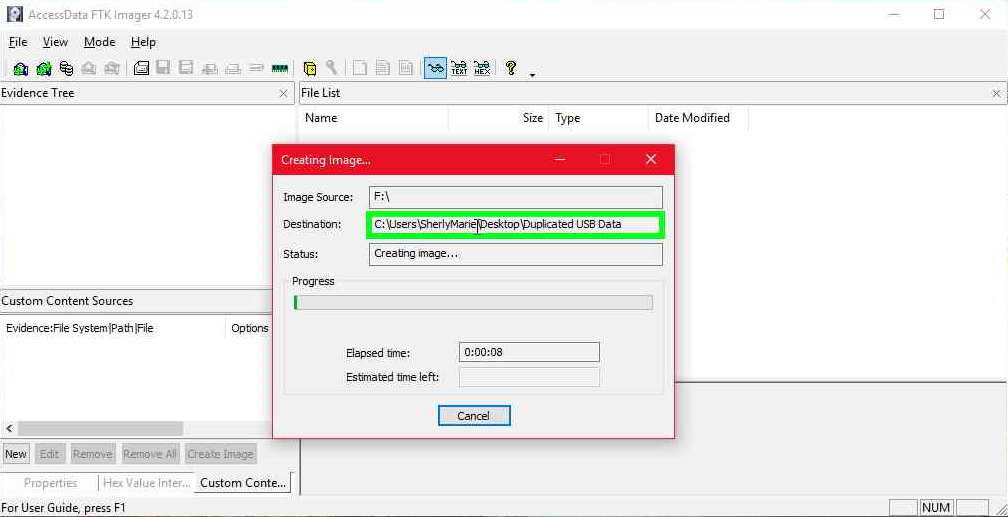


Figura 22. Preparación de archivos para analizar el caso

Según se presenta en la Figura 23, se procede con la creación de la imagen.

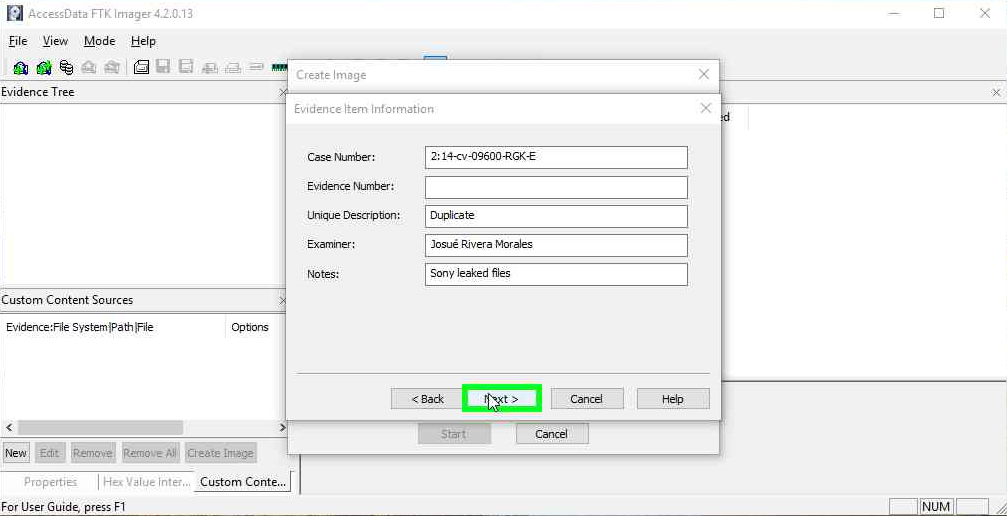
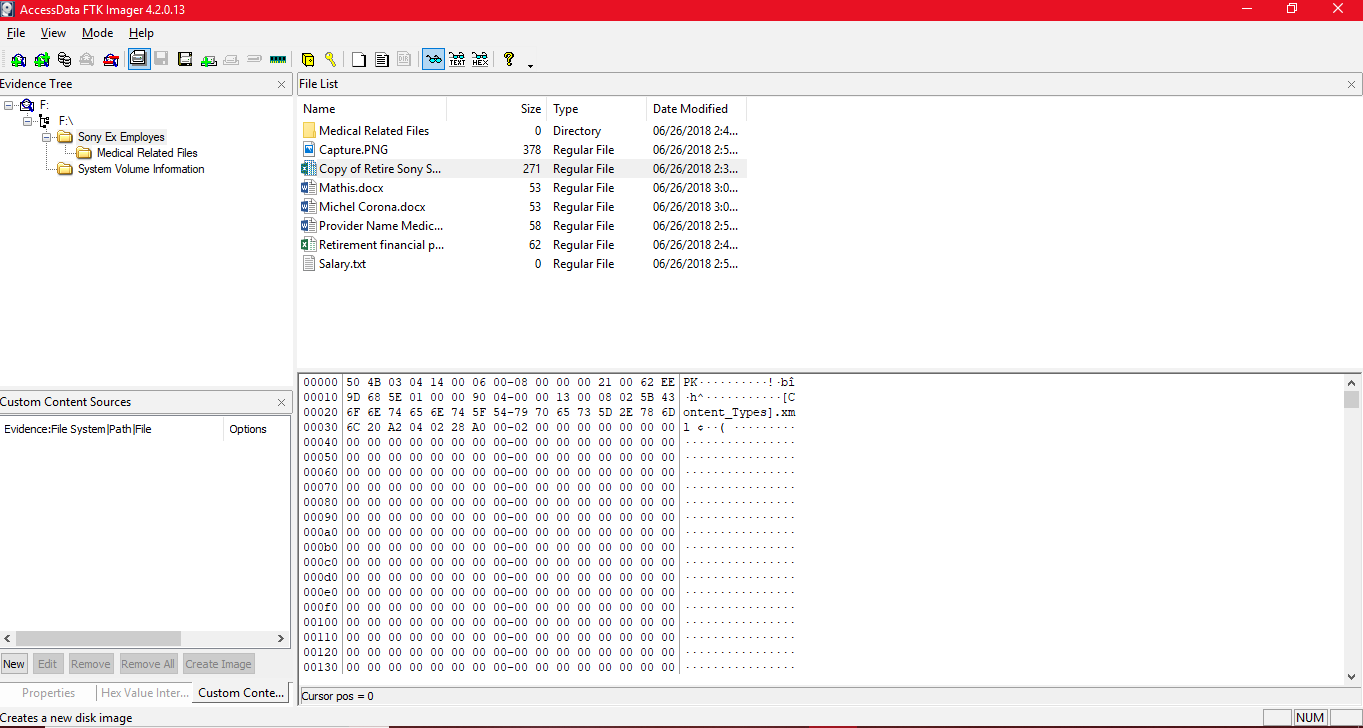


Figura 23. Creación de la imagen

La Figura 24 presenta como al culminar la creación de la imagen se pudo encontrar evidencia relevante al caso. Dentro de la información que contenía el USB se encontró un archivo nombrado ex empleados que contaba con un sinnúmero de datos personales de exempleados como lo son los demandantes. En este archivo podemos encontrar seguros sociales, salarios, email, cuentas de retiro, información médica, información familiar, razón de renuncia, en fin, todos los datos personales recolectados por Sony. Claramente podemos culpar a Sony por los daños ocasionados a los demandantes y a sus familiares. Imagen de los documentos que se encontraban dentro del archivo de exempleados.

 Figura 24. Documentos y archivos sobre exempleados

En la imagen de la Figura 25 puede observarse una lista de exempleados de Sony en la cual se presentan seguros sociales, fechas de nacimiento y nombre con apellido en la que se incluyendo la información de los demandantes.

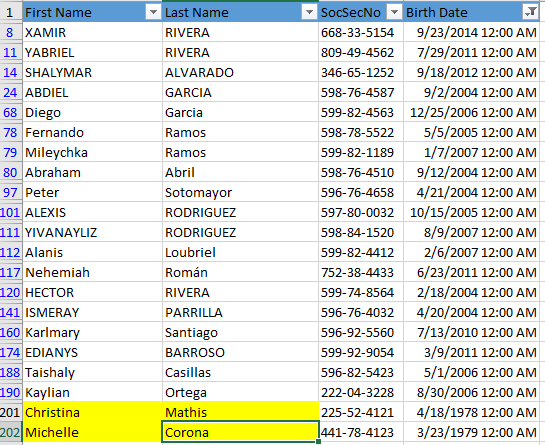
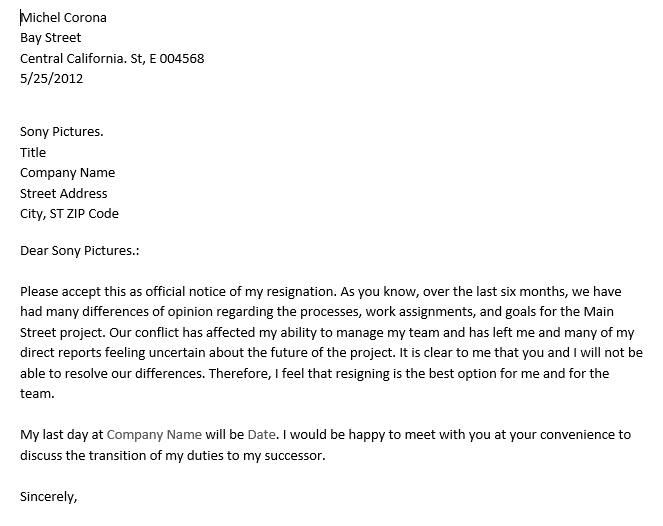
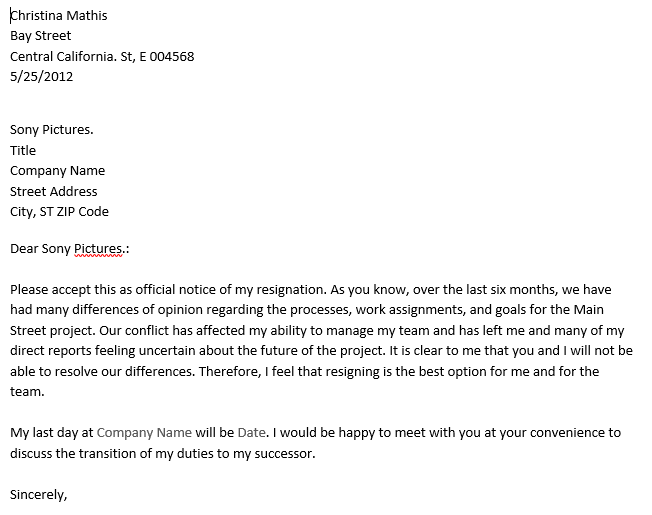


Figura 25. Información personal de los demandantes difundida al público

En las imágenes anteriores de la Figura 26 puede observarse las cartas de renuncias de los demandantes.

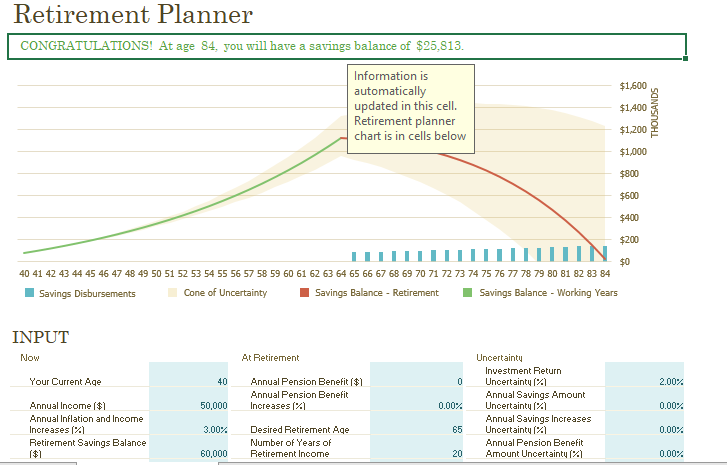


 Figura 26. Cartas de renuncia de los demandantes expuestas por los hackers.

En la Figura 27 puede verse información de citas médicas del personal de Sony Entertainment divulgado por los hackers.

 Figura 27. Itinerario de citas médicas expuesto

En la Figura 28 se observan informes del plan de retiro de la compañía Sony que fueron divulgados por los hackers.



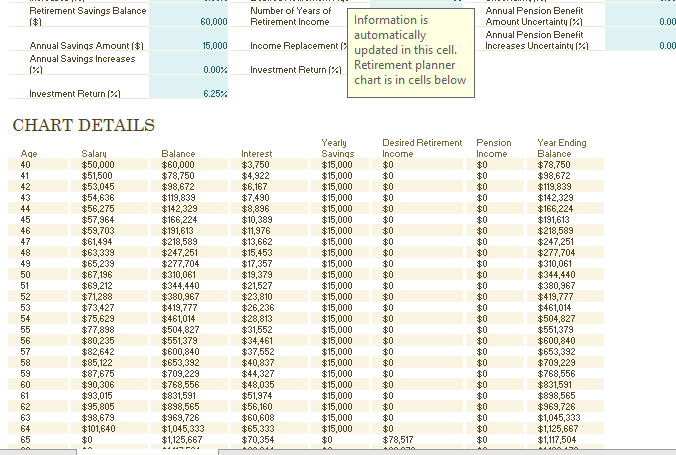


Figura 28. Informes sobre planes de retiro

.

**Conclusión**

Por lo que hemos analizado y la gran cantidad de datos personales de los demandantes presentes en el dispositivo de almacenamiento podemos encontrar un vínculo directo con Sony Pictures Entertainment Inc., por los daños sufridos a los demandantes. Se observa en la Figura 25 la información personal de los demandantes en específico su información sobre el número de Seguro Social, ya con la publicación de esta información el robo de su identidad fue inevitable.

**SECCIÓN 5: DISCUSIÓN DEL CASO**

Por lo que hemos estudiado del caso podemos ver que la insuficiencia de monitoreo, registros de auditoría, cifrado, uso controlado de credenciales administrativas y respuesta a incidentes contribuyeron a la violación masiva de la compañía. Para Sony Pictures Entertainment Inc., el solo mejorar su sistema de seguridad no será suficiente para reparar todos los daños que se han mencionado en este caso. Sin embargo, los delitos en la red además de que existen en todas partes, este análisis se realiza para llegar a un camino más claro para que los especialistas en seguridad mejoren la calidad de su trabajo dentro de la misma compañía. Al esto mejorar y tener el respaldo de un nivel más alto de compromiso con la misma organización le añade seguridad como un atributo a las funciones cotidianas de todos los que se involucran. No tan solo Sony, sino que todas las compañías y/o negocios deben conocer sus deficiencias y establecer componentes y elementos que sean procesables para poder mejorar constantemente. Las compañías, además de mejorar sus sistemas de seguridad también deberían tener un protocolo en el cual puedan auditar esos cambios para poder medir y ver cuán efectivos son esos cambios.

**SECCIÓN 6: AUDITORÍA Y PREVENCIÓN**

A través de este estudio se observa que existen varios delitos cibernéticos asociados con la comunicación en la web y el almacenamiento en la nube, pero la investigación se centrará en el tema de la seguridad de los sistemas de la compañía a partir de la historia del “hack” de Sony. Algunos de los obstáculos y limitaciones del estudio son que la investigación se basa en la información proporcionada por varios lugares de la web y algunos periódicos. El proceso de auditoría se llevó a cabo con el fin de hacer un análisis sobre los casos de seguridad y los distintos negocios en la seguridad de la compañía relacionados al “hack”, a su vez se revisó la literatura sobre investigaciones o casos relacionados con el mismo para hallar algún tipo de solución a este problema. Todo este proceso se lleva a cabo con el fin de crear un ambiente más seguro en el sentido de privacidad de la información y la seguridad del mismo frente a los diferentes ataques y/o amenazas que el mismo pueda enfrentar. Ya podemos ver a través del caso que algunos de los hallazgos fueron:

1. Sony tenía una falla en los controles de seguridad en varias áreas.
2. La compañía tenía un inventario bajo en dispositivos autorizados y no autorizados.
3. La defensa de su malware era insuficiente dentro de su sistema.
4. La estructura era muy deficiente en el sentido de la seguridad para los diferentes dispositivos de las redes como firewall, enrutadores e interruptores.

Algunas de las sugerencias para mejorar el sistema los son:

1. Hacer un análisis a los datos y/o información sensible que requiera de controles de cifrados e integridad por dicha información.
2. Un monitoreo constante de la información que entra y sale de la compañía y que detecte cualquier uso no autorizado de encriptación.
3. Limitar el acceso de uso de dispositivos externos a todo personal que tengan la necesidad de utilizarlos comercialmente. De ser necesario el mismo deberá ser monitoreado.
4. Crear una herramienta que detecte la información sensible (es decir, información personal, número de seguro social, información médica, etc.) utilizando palabras claves u otras características para descubrir intentos de extraer esta información sin autorización, a su vez limitando las redes y hacer bloqueos de dichas transferencias enviando a su vez una alerta al personal de seguridad encargado de toda esta información importante.
5. Utilizar un antimalware que sea basado en la red para poder identificar y ejecutar el tráfico no autorizado de las redes y que se utilice diferentes técnicas de detención basadas en firmas para poder identificar y poder tener acceso al contenido malicioso.
6. Mantener constancia de que cada sistema haga un “backup” semanalmente y si es posible que sea más frecuente para los sistemas que guardan la información confidencial.
7. Utilizar diferentes contraseñas o autenticación multifactor para todos los accesos administrativos incluyendo el dominio.
8. Hacer prácticas o pruebas periódicas de penetración externa e internas al sistema para identificar las vulnerabilidades del mismo y saber cómo llegar a un control más detallado.
9. Mantener al personal encargado al día con seminarios para que los mismo puedan detectar cualquier anomalía en el sistema y de encontrar uno poder realizar el procedimiento correcto ante cualquier ataque.

**SECCIÓN 7: CONCLUSIÓN**

En base de lo estudiado durante la maestría, he aprendido y el podido observar y estudiar que los crímenes cibernéticos son unos que siguen incrementando y que los criminales continúan en la búsqueda de nuevas y diferentes formas de poder cometer sus crímenes con el pensamiento de que jamás serán capturados o descubiertos. En base a estos crímenes podemos ver las diferentes vulnerabilidades de los sistemas y/o programaciones de las compañías o agencias, lo que hace de estas un punto muy frágil, ya que a través de estos crímenes se puede cometer fraudes lo que lleva a las agencias y/o compañías a tener problemas con diferentes agencias tanto estatales como federales. Es de cierta forma lamentable que estos problemas sucedan pongan en riesgo y comprometan a personas totalmente inocentes y que no tienen ningún tipo de relevancia con los fraudes que se cometen. También es importante recalcar la falta de leyes para proteger a las personas que son víctimas de estos ataques, ya sea por falta de evidencia o porque simplemente no se pueda encontrar una persona que sea la encargada del fraude. Por otra parte, estoy más que satisfecho con lo aprendido durante esta maestría y lo que he podido aprender realizando este proyecto. Gracias a la ayuda de los profesores y los cursos tomados sé que estoy más que preparado para cualquier caso que me toque enfrentar en mi carrera profesional. Tengo como norte, el poder educar a las personas y poder mostrarles las diferentes formas de que no sean víctimas de casos como el que se acaba de presentar. La seguridad y la educación a los ciudadanos es algo primordial. Entiendo que de cierta forma se deben implementar nuevas leyes que respalde nuestro trabajo como auditores y especialistas en el campo de la tecnología, ayudándonos a poder poner en práctica las técnicas y el material aprendido en clase y a su vez logrando evitar que sigan incrementando los crímenes cibernéticos.

**SECCIÓN 8: REFERENCIAS**

Abrahams, R. (2017). Target to Pay $18.5 Million to 47 States in Security Breach Settlement. *New York Times.* Retrieved from, https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html

Andy. (2014). *Sony movies leak online after hack attack.* Recuperado de, https://torrentfreak.com/sony-movies-leak-online-after-hack-attack-141129/

California Legislative Information. (2017). *State of California civil code section 1798.82*. *Amended by Stats. 2016, Ch. 337, Sec. 2*. *(AB 2828*). Retrieved from, https://leginfo.legislature.ca.gov/faces/codes\_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82

CONDUSEF. (2017). *El fraude cibernético*. Recuperado de, https://www.gob.mx/condusef/acciones-y-programas/el-fraude-cibernetico

Court Listener. (2014). *Michael Corona v. Sony Pictures Entertainment, Inc. (2:14-cv-09600)*. California: District Court, C.D. Retrieved from, https://www.courtlistener.com/docket/4152309/michael-corona-v-sony-pictures-entertainment-inc/

Hornyak, T. (2014*). It's now or never for Sony, says CEO*. Retrieved from, https://www.cio.com/article/2376068/consumer-technology/it-s-now-or-never-for-sony--says-ceo.html

Imrich, I. (2014). *Michael Corona and Christina Mathis v. Sony Pictures Entertainment, Inc. [re Data Breaches] class action complaint*. JDSupra. Retrieved from, https://www.jdsupra.com/legalnews/class-action-complaint-michael-corona-a-28715/

Judicial Council of California. (2018). *Robo de identidad, delitos financieros y delitos cibernéticos*. Cortes de California: La rama judicial de California. Recuperado de, http://www.courts.ca.gov/24642.htm?rdeLocaleAttr=es

Justia Dockets & Filing. (2018). *Michael Corona et al v. Sony Pictures Entertainment, Inc.* Recuperado de, https://dockets.justia.com/docket/california/cacdce/2:2014cv09600/606414

Law360. (2014). *Michael Corona et al v. Sony Pictures Entertainment, Inc*. Retrieved from, https://www.law360.com/cases/5490145d8d3fdf05ad000003

Leagle. (2015). *Corona V. Sony Pictures Entertainment Inc.* Retrieved from, https://www.leagle.com/decision/infdco20150602984

LIS Virginia Law. (2018). *Code of Virginia 18.2-186.6. Breach of personal information notification.* Retrieved from, https://law.lis.virginia.gov/vacode/18.2-186.6/

Merritt. (2016). *Symantec Corporation Identity theft primer*. Retrieved from Norton: http://mx.norton.com/identity-theft-primer/article

Norton Symantec. (2016). *What is identity theft?* Retrieved from, https://us.norton.com/internetsecurity-id-theft-what-is-identity-theft.html

Recovery Labs Division Computer Forensic. (2015). *Tipos de delitos informáticos. Clasificación según el “Convenio sobre la Ciberdelincuencia” de 1 de noviembre de 2001*. Recuperado de, http://www.delitosinformaticos.info/delitos\_informaticos/tipos\_delitos.html

RiskBased Security. (2014). *A breakdown and analysis of the December, 2014 Sony hack*. Retrieved from, https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

Schroeder, S. (2014). *Massive hack takes down Sony Pictures' computer system*. Retrieved from, https://mashable.com/2014/11/25/hack-sony-pictures/#v0j1HXbC.Pqw

Warren, C. (2014). *7 secrets from the Sony hack: Scripts, salaries, employee romances and more*. Retrieved from, https://mashable.com/2014/12/04/sony-hack-data-details/#Dibrd9jlzkq8

Waterstechnology.com. (2015). Cyber attach history: On everyones’s radar*. Waterstehnology.com*, 12-16.