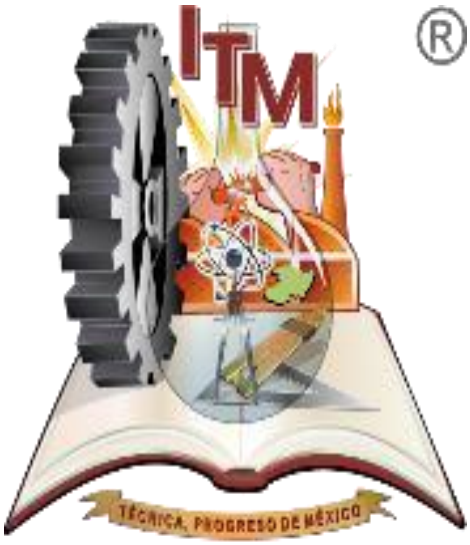
**INSTITUTO TECNOLÓGICO DE MORELIA**




# INVESTIGACIÓN SOBRE CASOS REALES DE PROBLEMAS LEGALES Y FRAUDES INFORMÁTICOS.

**ALUMNO:**

**ROBERTO HERRERA ORTIZ**

**PROFESORA:**

**KENIA ALINE AYALA ROBLES**

**Auditoría en Tecnologías de la Información.**

**19 de abril del 2021**

# Contenido

## Casos reales de problemas legales de la auditoría para analizar y proponer soluciones:

# EL FRAUDE MILLONARIO EN BANORTE:

**¿Quién es el atacante?**

R= Salinas y un funcionario de Banorte.

**¿Con qué organización y/o grupo está asociado el atacante?**

R= Grupo Salinas.

**¿Cuál es el motivo del atacante?**

R= Defraudó a una treintena de clientes de la Casa de Bolsa de Banorte Ixe por un monto de 500 millones de pesos.

**¿Qué método de ataque se utilizó?**

R= Se expedían documentos idénticos a los del banco para después dárselos a sus clientes, como por ejemplo contratos y estados de cuenta, pero dichos documentos eran completamente falsos. Salinas se dedicó a engañar a sus clientes por años con este método, pero la realidad es que las cuentas jamás se aperturaron. Salinas fue tomando dinero poco a poco para no levantar sospechas, en especial aquellos que no tenían acceso a internet y que estaban confiados en los documentos que habían estado recibiendo de la institución.

**¿Cómo se podría prevenir o mitigar este ataque?**

Quedarse siempre con una copia del contrato y verificar que éste sea oficial, revisando que esté inscrito en el Registro de Contratos de Adhesión (RECA) en la página de la Condusef.

Verificar que los estados de cuenta cuenten con todos los elementos necesarios: que coincidan desde el tipo de letra hasta los movimientos realizados e incluyan logo del banco y teléfonos de atención.

Una institución financiera no solicita hacer depósitos a cuentas personales de otro individuo o instituciones y que es importante guardar recibos o hacer transferencias, que dejan huella y pueden ser rastreadas, ya que estos elementos pueden servir posteriormente como comprobantes de los movimientos.

## Casos reales de fraudes informáticos y proponer controles para prevenirlos lo siguiente:

# 1.- Home Depot

**¿Quién es el atacante?**

**R=** WannaCry.

**¿Con qué organización y/o grupo está asociado el atacante?**

**R=** Equation Group.

**¿Cuál es el motivo del atacante?**

**R=** Los archivos del usuario se mantuvieron retenidos y se solicitó un rescate en bitcoins para su devolución.

**¿Qué método de ataque se utilizó?**

**R=** Ransomware de cifrado.

**¿Qué objetivo y vulnerabilidades se utilizaron contra la empresa?**

**R=** Los cibercriminales responsables del ataque aprovecharon una debilidad en el sistema operativo Microsoft Windows mediante un ataque, conocido como EternalBlue. Mediante el exploit, los malos pudieron obtener acceso remoto a los ordenadores e instalar el cifrador.

**¿Cómo se podría prevenir o mitigar este ataque?**

**R=** 1) Instala las actualizaciones de seguridad. 2) Crea copias de seguridad de forma regular y guárdalas en dispositivos que no estén conectados al ordenador constantemente. 3) Usa un antivirus de confianza.

# 2.- YAHOO

**a. ¿Quién es el atacante?**

**R=** Michael Calse.

**b. ¿Con qué organización y/o grupo está asociado el atacante?**

**R=** Se autodenomina MafiaBoy.

**c. ¿Cuál es el motivo del atacante?**

**R=** Dejar fuera de servicio a Yahoo por un par de horas, sino que también quiso probar su ataque con e-bay y Amazon, empresas que reportaron pérdidas por más de 1.2 millones de dólares, tras la inminente caída de sus respectivos sitios web.

**d. ¿Qué método de ataque se utilizó?**

**R=** Ejecutó un ataque DOS/DDOS (Link a descripción).

**e. ¿Qué objetivo y vulnerabilidades se utilizaron contra la empresa?**

**R=** Los atacantes suelen generar grandes volúmenes de paquetes o requerimientos para, finalmente, sobrecargar el sistema objetivo. En el caso de un ataque de denegación de servicio distribuidos (DDoS) el atacante utiliza múltiples fuentes de vulnerabilidad o fuentes controladas para generar el ataque. En general, los ataques DDoS pueden ser segregados según la capa del modelo de interconexión de sistemas abiertos (OSI) que atacan.

**f. ¿Cómo se podría prevenir o mitigar este ataque?**

**R=** Implemente firewalls para ataques sofisticados de aplicaciones. Conocer qué es el tráfico normal y anormal. Reduzca la superficie expuesta a ataques

# CONCLUSIÓN

En conclusión, la ciberseguridad se basa en que estas personas no puedan hackearnos y, por ende, hacer que les cueste demasiado poder vulnerar nuestro sistema, además de que la ciberseguridad ayuda a reaccionar de forma adecuada en el caso de que se constate que se ha producido un ataque. Además, la auditoría nos ayuda a esclarecer lo bueno o lo malo que este dentro de una empresa, con el fin de que no ocurran incidentes como algunos de los que se muestran en el documento y que las personas se sientan seguras de donde ponen su información y/o bienes. La ciberseguridad es extremadamente importante, ya que todos tenemos acceso a internet y mucha de nuestra e información está en ella, así que va haber personas que quieran robar nuestra información para hacer mal uso de la misma o para poder vulnerar nuestra red y poder saber qué es lo que estamos haciendo en ese preciso momento.

# BIBLIOGRAFÍA

Sofecom. (2017, febrero 20). Los ataques cibernéticos a empresas más famosos de la historia. Recuperado el 19 de abril de 2021, de Sofecom.com website: https://sofecom.com/ataques-ciberneticos-empresas/

de América-Redacción, V. (s/f). Home Depot confirma incursión de “hackers”. Recuperado el 19 de abril de 2021, de Vozdeamerica.com website: https://www.vozdeamerica.com/economia-finanzas/home-depot-robo-identidad-cibernetico-tarjetas-clientes

El Fraude Millonario en Banorte. (s/f). Recuperado el 19 de abril de 2021, de Scribd.com website: https://es.scribd.com/document/399004562/El-Fraude-Millonario-en-Banorte