
VNIVERSIDAD NACIONAL
AVTÓNOMA DE
MEXICO

# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN

## ANÁLISIS Y PROPUESTA DE SEGURIDAD PARA SISTEMAS DE BANCA MÓVIL MEDIANTE ÁRBOLES DE ATAQUE

**TESIS**
**QUE PARA OPTAR POR EL GRADO DE:**
**MAESTRO EN INGENIERÍA (COMPUTACIÓN)**

**PRESENTA:**
**LUIS HUGO FLORES ROMÁN**

**DIRECTOR DE TESIS**
**DR. ENRIQUE DALTABUIT GODAS**
**DGTIC - UNAM**

**MÉXICO, D. F. MARZO 2014**

# Agradecimientos

A la Universidad Nacional Autónoma de México, por otorgarme la oportunidad de seguir formando parte de su comunidad.

Al Dr. Enrique Daltabuit Godas, por su paciente y alentadora conducción.

A mis profesores dentro del Posgrado en Ciencia e Ingeniería de la Computación, por su interés y dedicación al transmitirme parte de sus conocimientos.

A mis sinodales, por dedicar parte de su valioso y limitado tiempo libre para mejorar este trabajo.

A mi familia, por su apoyo, motivación e insistencia.

A mis compañeros y amigos.

Muchas gracias.

# Contenido

# Introducción

En los últimos años, la penetración y el uso del internet han ido en aumento, así como la variedad de aplicaciones que pueden darse a este medio de comunicación. A pesar de que para muchos el internet es sólo una fuente de información y el temor a ser víctima de algún tipo de fraude electrónico es latente, poco a poco los usuarios han comenzado a considerar otro tipo de servicios, como el de la banca electrónica.

Si bien el método tradicional de acceso a este tipo de productos ha sido las computadoras personales, la gran penetración de los dispositivos móviles ha obligado a que las instituciones financieras instancien igualmente sus servicios en estas nuevas plataformas, dando origen a la banca móvil.

Su utilización representa grandes beneficios tanto para clientes como para instituciones. Los cuentahabientes pueden utilizarlos fuera de los horarios de servicio tradicionales, pueden realizar transacciones locales e internacionales desde cualquier lugar, reduce la utilización de dinero en efectivo y, en consecuencia, reduce el riesgo de sufrir un robo. Por otro lado, le da la oportunidad a los bancos de penetrar en nuevos mercados a través de nuevos canales de distribución, además de reducir sus costos de operación.

Sin embargo, la migración de los servicios bancarios tradicionales hacia estos nuevos paradigmas expone tanto a cuentahabientes como a instituciones a nuevos riesgos de diversa naturaleza, mismos que deben ser atendidos para mantener la seguridad y la exactitud en las transacciones (así como la percepción de las mismas en el usuario), lo que constituye un factor crítico en el éxito y crecimiento de la banca electrónica.

En este sentido, si bien las instituciones bancarias establecen los controles pertinentes para proteger a sus usuarios de las amenazas más críticas, el hecho de que suelen priorizar la funcionalidad de los sistemas sobre su seguridad es igualmente una realidad.

Siendo así, ¿Tales amenazas están realmente cubiertas?

Este trabajo busca responder a la pregunta anterior mediante la realización de un análisis del riesgo al uso de la banca electrónica/móvil a través de árboles de ataque, los cuales permiten modelar las amenazas a las que un sistema se encuentra expuesto, calcular su impacto y determinar la necesidad de adoptar medidas preventivas. Esta técnica, formal y metódica, se origina con la identificación de una meta principal a alcanzar dentro del sistema en estudio y de todos los posibles ataques que contribuyan a lograr tal objetivo que, en este caso, consiste en acceder de manera no autorizada a una consulta o transacción en la cuenta de un usuario.

Para llegar a ese punto, se parte de conceptos muy generales hasta alcanzar otros muy específicos, considerando la estructura siguiente:

En los primeros dos capítulos se realiza una descripción general de la banca electrónica y de su seguridad, incluyendo dentro de ésta tanto vulnerabilidades y ataques a los que están expuestos con mayor frecuencia, así como las medidas genéricas que normalmente se establecen para mitigar sus riesgos.

Posteriormente, en el capítulo tres, se lleva a cabo un recorrido por las metodologías de análisis de riesgos, con un enfoque hacia los árboles analíticos y de ataque, como antesala a uno de los análisis principales en este trabajo.

A continuación se aplica una metodología de análisis de riesgos, basada en árboles de ataque, al uso de la banca electrónica. Los resultados obtenidos son confrontados con las medidas de seguridad implementadas por cinco de los principales bancos mexicanos, buscando en última instancia verificar la efectividad de tales soluciones o identificar vectores aún explotables por un atacante. Así mismo, las reflexiones emanadas de este ejercicio son consideradas en capítulos subsiguientes, referentes a banca móvil, para realizar una comparativa de las problemáticas asociadas a las diferentes plataformas.

Finalmente, en los capítulos cinco y seis, se describe con un mayor detalle la subcategoría de banca móvil, retomando posteriormente las actividades de análisis del riesgo contextualizadas en las plataformas inalámbricas.

Una vez analizados los resultados de los diferentes análisis, se señalan algunas consideraciones finales en las que además de comparar e interpretar la información obtenida, se realizan algunas propuestas de mejora, a modo de conclusión, a los controles de seguridad evaluados.

# 1. Banca electrónica

La banca electrónica se define como el envío automatizado de información y servicios bancarios, tanto tradicionales como novedosos, directamente al consumidor a través de medios de comunicación electrónicos e interactivos, como computadoras personales, teléfonos y teléfonos móviles [1].

Forma parte, en conjunto con las aseguradoras e intermediarios[1] en línea, de los servicios financieros electrónicos, que a su vez se encuentran incrustados de manera general en el comercio electrónico.

Su adopción se ha generalizado en los bancos de diversas partes del mundo y, si bien en el caso mexicano aún no se encuentra arraigado en su totalidad entre los usuarios, su utilización va en aumento. En la actualidad existen alrededor de 40 millones de internautas, de los cuales 26 millones son mayores de edad y 21 millones de éstos cuentan con algún producto bancario[2]. En 2012, 12 millones de estos usuarios bancarizados realizaron transacciones a través de la banca electrónica de manera regular (2 millones más que en 2011) y 41% de éstos las comenzaron a realizar hacía un año o menos (16% más que en 2011). A su vez, los cuentahabientes que realizan visitas a las sucursales bancarias varias veces a la semana han caído a un 1% (9% menos que en 2011) [2], números que confirman la tendencia a la alza en la utilización de este tipo de servicios.

## 1.1 Tipos de banca electrónica

Con el fin de brindar el mejor servicio posible a sus cuentahabientes, los bancos suelen utilizar combinaciones de medios electrónicos de acuerdo al tipo de cliente, al tipo de operaciones que éste realiza y a los productos con los que cuenta. Por tal razón, la banca electrónica suele clasificarse de acuerdo al tipo de medio utilizado.

### 1.1.1 Utilizando una conexión telefónica

Comenzó a surgir al final de los años 60 y creció a pasos agigantados hasta consolidarse a principios de los 70 [1]. La interacción inicial, utilizando una línea telefónica clásica, consistía en la comunicación con un ejecutivo bancario que realizaba las transacciones a nombre del cuentahabiente, o en la comunicación directa con una terminal automática, sin embargo, a finales del siglo veinte los teléfonos móviles comenzaron a involucrarse de igual manera en los servicios bancarios a través de mensajes SMS[3]. Con la llegada de los teléfonos inteligentes, la banca a través de GSM[4] e internet móvil[5] se convirtió en un componente esencial de la banca electrónica.

[1] Entidad que arregla una transacción entre comprador y vendedor, obteniendo una comisión cuando ésta se lleva a cabo exitosamente.
[2] Cuenta de nómina, de ahorros, tarjetas de crédito o débito, etc.
[3] Short Message Service. Servicio para enviar mensajes de texto cortos entre teléfonos fijos o móviles, utilizando protocolos estandarizados.
[4] Global System for Mobile Communications. Set de estándares que describe los protocolos para la segunda generación de redes celulares digitales, utilizada por los teléfonos móviles.
[5] Internet a través de un proveedor de servicio de teléfonos celulares. Para ser considerado internet móvil, un dispositivo debe obtener sus servicios de voz o datos directamente de las antenas base de su proveedor, no por Wi-Fi.

#### *1.1.1.1 Banca telefónica*

- A través de un ejecutivo. Consiste en la comunicación con un empleado del banco a través de una línea telefónica clásica, quien provee información de servicios y productos bancarios al cliente, además de ejecutar operaciones en su cuenta tras una correcta identificación mutua. Cuenta con la ventaja de requerir únicamente un teléfono, aunque para la institución bancaria representa un gasto extra al tener que contratar a un empleado exclusivamente para esta función o una menor productividad al distraer de sus actividades diarias a uno ya existente para proveer este servicio.

- Sistema telefónico automatizado. Requiere la utilización de un teléfono de tonos. Consiste en la comunicación directa con una terminal automática, la cual provee menús interactivos en los que se puede navegar por un árbol de opciones sencillo usando los botones del teléfono. Recibos o información más detallada pueden ser enviados al cuentahabiente vía fax. Uno de sus inconvenientes surge cuando el cliente no puede seleccionar una opción correcta o las respuestas del sistema no van de acuerdo a sus deseos, por lo que en muchos casos es necesario conectar este servicio con ejecutivos bancarios, lo que representa un doble gasto para la institución.

La autenticación[6] que se efectúa al utilizarse este tipo de banca se da en forma de un número personal (generalmente un número de tarjeta de crédito) y una contraseña numérica para confirmar transacciones, que el cliente comunica al ejecutivo o a la terminal automatizada. El riesgo de lo anterior radica en que cualquier persona que adquiera conocimiento sobre estos dos identificadores será capaz de realizar cualquier tipo de movimiento sin el consentimiento del titular, por lo que una autenticación multifactor[7] siempre es recomendada.

#### *1.1.1.2 Banca móvil*

Se realiza a través de una conexión telefónica inalámbrica, utilizando teléfonos celulares y teléfonos inteligentes. Una descripción más detallada sobre las características de este tipo de banca electrónica puede ser consultada en el capítulo cinco de este trabajo.

### 1.1.2 Utilizando una computadora personal

A pesar de la gran proliferación de los teléfonos inteligentes, la banca a través de computadoras personales con conexión a internet aún tiene un rol muy importante en el día a día actual de la banca electrónica. Se divide en banca en casa, a través de internet y a través de correo electrónico.

- Banca en casa. Requiere la instalación de una aplicación cliente en una computadora personal seleccionada por adelantado, generalmente en casa u oficina, exclusivamente a través de la cual el cuentahabiente pude acceder a los servicios bancarios. Del lado del banco, un servidor atiende las peticiones de los clientes previa verificación de identidades, ejecuta transacciones, además de generar y enviar recibos digitales a los usuarios.

[6] Es el acto de confirmar la veracidad de un atributo, dato o entidad.

[7] Requiere la presentación de dos o más de los tres factores de autenticación existentes: algo que el usuario sabe, algo que el usuario tiene o algo que el usuario es.

La aplicación cliente es generalmente multiusuario, por lo que pueden definirse varias cuentas con diferentes roles y permisos.

- Banca por internet. Puede ser utilizada en cualquier ubicación con una conexión a internet. A diferencia de la banca en casa, no es necesaria la utilización de una computadora seleccionada por adelantado para acceder a los servicios bancarios, sino que basta con un navegador web con el que se visita el portal bancario de la institución financiera y, después de la verificación de identidad, pueden ejecutarse transacciones y consultas.

  Esta modalidad no es exclusiva de computadoras personales, ya que los teléfonos inteligentes cuentan con la funcionalidad de conectarse a internet tanto por Wi-Fi como a través de internet móvil, utilizando igualmente un navegador web.

- A través de correo electrónico. De manera similar al servicio de notificación vía SMS, algunos bancos pueden ofrecer información al cliente acerca del estado de su cuenta a través de correo electrónico. Debido a que es un canal de comunicación independiente al banco y a la sensibilidad de la información que puede generarse, no se realizan otro tipo de transacciones por este medio.

### 1.1.3 Zonas de autoservicio

Además de las ya mencionadas, otra forma de banca electrónica ampliamente conocida es aquella establecida en zonas de autoservicio, donde las ATM[8] se encuentran a disposición de los cuentahabientes.

Debido a las altas demandas de procesamiento y a la disminución en su costo, estos dispositivos han migrado de las construcciones personalizadas a base de microprocesadores y circuitos integrados a arquitecturas similares a las de las computadoras personales, utilizando periféricos y sistemas operativos afines, además de comunicaciones Ethernet e IP a través de las cuales establecen conexión con la red compartida de ATMs[9] [3].

Estos dispositivos funcionan las 24 horas del día y se encuentran disponibles tanto en zonas adjuntas a los bancos como en lugares alternativos con importantes flujos de personas. Inicialmente ofrecían únicamente el retiro de efectivo con cargo a la cuenta de cada cliente y la consulta de saldos, sin embargo, en la actualidad su gama de servicios incluye depósitos, transferencias, pago de servicios a terceros, etc. Para su utilización es necesaria una tarjeta de crédito o débito, además de su PIN asociado.

## 1.2 Servicios de banca electrónica

Aunque los servicios y arquitecturas ofrecidos varían de país a país y de banco en banco, las consultas y transacciones más comúnmente solicitadas son las equivalentes, por

[8] Automated Teller Machine. Dispositivo computarizado que permite a los clientes de una institución financiera ejecutar transacciones sin la necesidad de un empleado bancario. Llamado comúnmente "cajero automático."

[9] En esta red, todos los cajeros automáticos (sin importar que sean de bancos distintos) se encuentran conectados a un equipo intermediario que tiene acceso a las bases de datos de todas las instituciones bancarias asociadas y direcciona las peticiones según corresponda, permitiendo al usuario el retiro de efectivo desde dispositivos distintos a los provistos por su banco.

internet, de aquellas que más se realizan en ventanillas o cajeros [4], con excepción del retiro o depósito de dinero en metálico.

### 1.2.1 Consultas

- Saldos en cuentas y productos contratados.
- Movimientos en cuentas y tarjetas de crédito o débito.
- Valoración de inversiones y rendimientos.
- Información de índices bursátiles y tipos de cambio.
- Estado de domiciliaciones[10].

### 1.2.2 Transacciones

- Apertura de nuevas cuentas.
- Transferencia entre cuentas.
- Compraventa de valores.
- Aportaciones extraordinarias a fondo de pensiones.
- Adición o supresión de domiciliaciones.

La gama de servicios disponibles sigue creciendo e, inclusive, en la actualidad el verdadero reto para las entidades financieras no consiste en ofrecer sus servicios tradicionales a través de internet, sino en diseñar servicios innovadores, quizá inexistentes fuera de línea, que les permitan la atracción de nuevos clientes y mercados.

## 1.3 Riesgos de la banca electrónica

La banca electrónica no sólo está expuesta a los mismos riesgos que su contraparte tradicional, sino que potencia algunos de ellos, como los aspectos regulatorios, legales, operacionales y de reputación [5], provocando que varios países modifiquen sus marcos legales para garantizar la seguridad y la solvencia de sus sistemas bancarios y de sus mercados, así como para proteger los derechos de los consumidores y la confianza de los ciudadanos en las instituciones financieras.

### 1.3.1 Riesgo legal y regulatorio

Los nuevos canales de comunicación le dan la oportunidad a los bancos de penetrar en mercados internacionales con mayor efectividad y rapidez, sin embargo, la falta de conocimiento de las leyes y regulaciones de cada nueva locación puede derivar en que los servicios que proveen sean causa de delitos involuntarios o que violen los derechos de los cuentahabientes. Por otro lado, la poca claridad en cuestiones de jurisdicción no sólo afecta las labores de regulación y supervisión a los bancos, sino que en el ámbito legal

[10] Cargo a una cuenta bancaria del pago a un recibo presentado por un tercero, por ejemplo, las cuentas telefónicas o de televisión por cable.

igualmente provoca dificultades al tratar de definir quién debe tomar acción ante actos delictivos.

Adicionalmente, el anonimato que brinda la banca electrónica puede facilitar el lavado de dinero, debido a que una vez abierta una cuenta es complicado verificar que sea el cuentahabiente el que está realizando las transacciones, por lo que muchas regulaciones insisten en la verificación constante de la identidad de todos los clientes bancarios y en el monitoreo de los movimientos realizados a través de internet.

### 1.3.2 Riesgo operacional

Se debe asegurar que los bancos cuentan con las prácticas adecuadas para garantizar la confidencialidad e integridad de los sistemas y los datos, que forman parte de los principales actores en este nuevo paradigma financiero. De igual manera, los equipos deben estar preparados para soportar un gran volumen de transacciones y tener mecanismos para la rápida recuperación de las actividades si alguna incidencia negativa se presentara. Debido a las características de estos nuevos servicios, la administración del riesgo operacional es una parte fundamental de la administración del riesgo global actual de la mayoría de las instituciones financieras.

### 1.3.3 Riesgo de daño a la reputación

Brechas en la seguridad o discontinuidad en los servicios no sólo dañan la reputación de un banco en específico, sino que dota a la banca electrónica en general de una percepción negativa entre los usuarios. Sin embargo, como estos efectos negativos pueden derivarse también de malas experiencias del cuentahabiente producto del desconocimiento de la necesidad de medidas de protección en la utilización de estos servicios, la administración del riesgo en la banca electrónica no sólo debe considerar regulaciones internas, sino campañas de educación sobre el buen uso de estos nuevos canales de comunicación.

Todas las problemáticas antes citadas obligan a una revisión tanto de los controles regulatorios, que deben mantenerse al día con una tecnología en constante cambio, como de las definiciones y permisos legales, como la redefinición de las fronteras entre las naciones.

De igual manera, se hace evidente que la colaboración entre los países es fundamental para evitar que vacíos legales o de jurisdicción faciliten actos ilícitos y, por último, que las nuevas formas de ofrecer servicios bancarios agregan las problemáticas de las tecnologías de la información a la agenda de las instituciones, las cuales ya no pueden preocuparse únicamente por cuestiones financieras.

# 2. Seguridad de la banca electrónica

Dentro de los principales riesgos inherentes a la banca electrónica, son los operacionales los que suscitan el mayor interés para la seguridad informática. Toda transacción comercial realizada a través de medios electrónicos requiere la presencia de cinco propiedades fundamentales para llevarse a cabo exitosamente [6, pp. 268, 269] [7]:

1. Integridad. Verificar si la información enviada o recibida a través de internet ha sido modificada o replicada[11] por un tercero no autorizado.

2. No repudio. Prevenir que los participantes en una transacción electrónica nieguen posteriormente las acciones realizadas.

3. Autenticidad. Identificar la identidad de los participantes en la transacción. El usuario debe estar seguro de que se comunica con el banco antes de enviar información sensible y el banco debe tener la certeza de que la información que procesa es la de su cuentahabiente.

4. Confidencialidad. Asegurar que el acceso a los datos enviados y recibidos sólo se encuentre disponible para aquellos autorizados para hacerlo. Adicionalmente, las instituciones financieras deben resguardar los datos personales, asociados a sus cuentas, de todos los usuarios.

5. Disponibilidad. Mantener en correcto funcionamiento todos los servicios bancarios electrónicos ofrecidos por la institución financiera.

Una brecha en cualquiera de estas propiedades representa un problema de seguridad y, en la actualidad, existen un gran número de acciones y herramientas destinadas a vulnerarlas.

## 2.1 Vulnerabilidades y ataques

Existen tres puntos susceptibles, en mayor o menor medida, a ser vulnerados durante una transacción de banca electrónica: redes y servicios bancarios, canales de comunicación y usuarios (Figura 1.)

[11] En un ataque de réplica una transmisión de datos legítima es interceptada (credenciales de acceso a un sitio, por ejemplo) para hacerla válida posteriormente por el atacante, quien reenvía los datos cuando una autenticación de usuario es requerida.

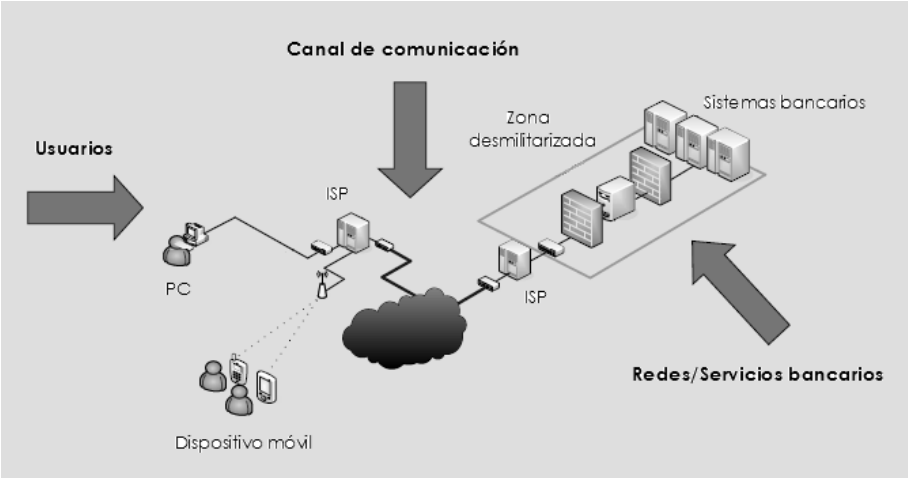


Figura 1. Puntos de control en la banca electrónica mediante computadoras personales[12].

### 2.1.1 Usuarios

De los puntos de control propuestos, es el factor humano el que en la mayoría de las ocasiones resulta más débil, debido principalmente a que la falta de educación en materia de seguridad en los medios electrónicos no les permite a los usuarios el tomar decisiones informadas, lo que los hace vulnerables a engaños de todo tipo.

Los esfuerzos de los atacantes en lo referente a los usuarios se enfocan en la obtención de las credenciales de acceso a los servicios de banca electrónica, lo cual puede ser logrado de diversas maneras.

#### *2.1.1.1 Código malicioso*

Son piezas de software que tienen la finalidad de realizar algún ataque. Aunque en el pasado varios de sus tipos sólo estaban diseñados para causar molestia en los usuarios o para dañar sus computadoras, en la actualidad la gran mayoría tiene motivaciones no legítimas, como el robo de información personal y financiera.

La cantidad de código malicioso existente está en aumento. En 2011, únicamente, se creó la tercera parte de las aproximadamente 88 millones de muestras conocidas [8], lo cual es en extremo preocupante debido a que los programas antivirus detectan alrededor de un 24% del código cuya creación es reciente.

Aunque en muchas ocasiones es erróneamente conocido de forma general como virus informático, lo cierto es que existen varios tipos de código malicioso, cada uno con características y finalidades distintas.

- Virus. Se trata de una pieza de software que tiene la habilidad de replicarse a sí misma adjuntándose a otros programas para, a través de la ejecución de los portadores, realizar las acciones para las que fue programado, que pueden ser tan benignas como mostrar un mensaje al usuario o tan malignas como borrar por completo la información contenida en un disco duro.

[12] Basada en la imagen "Puntos de control" de Benjamín Bernal Díaz, contenida en "La Seguridad en la Banca y Comercio Electrónico", página 9. Ponencia perteneciente al Día Internacional de la Seguridad en Cómputo 2009 en México.

- Gusanos. Al igual que los virus pueden replicarse a sí mismos, con la diferencia de que lo hacen de computadora a computadora y no de archivo a archivo. Su principal función destructiva es la de consumir recursos de un equipo (memoria) o de la red en la que se encuentra (ancho de banda.)

- Caballos de Troya. De manera similar a lo acontecido en la Ilíada de Homero, esta pieza de software se le presenta a la víctima como algo legítimo e inofensivo, aunque esconde en realidad código malicioso en su interior. Su ejecución es obra del propio usuario y es la vía de descarga e instalación de virus, puertas traseras[13] y rootkits[14], entre otros. A diferencia de los virus y gusanos, los caballos de Troya carecen de la habilidad de replicarse.

  Este tipo de código malicioso es el de mayor incidencia en las infecciones detectadas en el último año, ya que el 66% de ellas resultaron ser caballos de Troya en el primer cuatrimestre del año 2012 [9].

- Bots. Código malicioso que, una vez instalado en una computadora, habilita a ésta para responder a las instrucciones remotas de un atacante, convirtiendo el equipo en una especie de zombi. Un gran número de bots controlados por la misma persona conforman una red de bots, cuyos recursos en conjunto pueden ser utilizados por un atacante para fabricar correo no deseado[15], robar información sensible de otros sistemas, realizar ataques de denegación de servicio distribuidos, entre otros (Figura 2.)

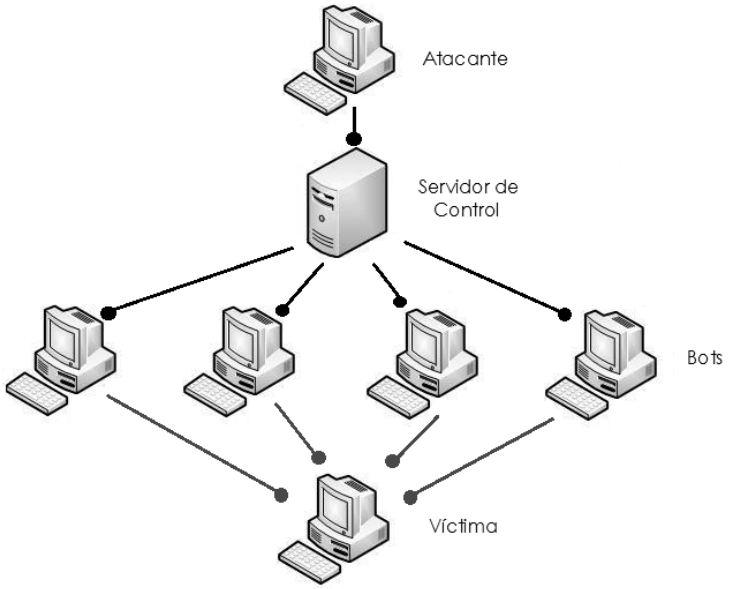


Figura 2. Diagrama básico de una red de bots.

[13] Es un método para obtener y mantener ilegalmente acceso remoto a algún sistema, evitando la autenticación y su detección en el mismo.
[14] Es software diseñado para ocultar la existencia de procesos o programas que otorguen acceso ilegal a un sistema como, por ejemplo, una puerta trasera.
[15] Es el uso de sistemas electrónicos de mensajería para enviar mensajes no solicitados, en muchas ocasiones publicidad, en gran volumen.

A pesar de que el número de redes de bots operando en el mundo no es conocido con certeza, entre finales del 2011 y principios del 2012 cientos de ellas fueron identificadas con aproximadamente 24 millones de computadoras capturadas en total, lo cual es muy preocupante por su capacidad de realizar ataques a gran escala y porque el 95% del correo no deseado y el 85% del código malicioso circulando a nivel mundial se distribuye a través de este medio [10].

De los tipos de código malicioso descritos, son los caballos de Troya y los bots los que con mayor frecuencia están relacionados con la realización de fraudes, ya que pueden ser utilizados para suplantar aplicaciones bancarias, para redirigir las conexiones a sitios web fraudulentos o para robar directamente información financiera y/o sensible de los usuarios, entre otras funcionalidades.

El código malicioso puede ser adquirido desde diversas fuentes: a través de la ejecución de archivos infectados, en un archivo adjunto a un correo electrónico, descargados desde sitios web maliciosos (con sólo acceder a ellos, deslizando el puntero del ratón o pulsando sobre áreas específicas), en redes punto-a-punto[16], contenidos en medios extraíbles (memorias USB, CD/DVD, discos duros), por vulnerabilidades en los sistemas operativos y aplicaciones, etc.

### *2.1.1.2 Suplantación*

Cualquier intento de un atacante por obtener información confidencial en una comunicación electrónica, haciéndose pasar por una entidad legítima, es denominado suplantación (phishing.) Esta actividad no emplea ningún tipo de código malicioso y basa su éxito en el engaño, el fraude, la ingeniería social[17].

A pesar de que la forma de suplantación más popular es realizada a través de correo electrónico, existen varias maneras de llevarla a cabo:

- Correo electrónico y sitios web. Consiste en el envío de un correo a nombre de instituciones financieras u otras compañías que solicita la confirmación de cuentas de usuario, a través de un enlace provisto en el propio mensaje. Al hacer clic en el mismo, el usuario es direccionado a una réplica de un sitio legítimo, controlado por el atacante, donde voluntariamente entrega información sensible (números de cuenta o tarjeta, credenciales de acceso, etc.) o descarga código malicioso a su equipo como consecuencia de su desconocimiento en lo concerniente a la seguridad.

  Millones de correos de este tipo son enviados cada día y, cuando algunas personas eventualmente caen en el engaño, sus cuentas de banco o incluso algunos aspectos de su identidad son robados electrónicamente para posteriormente ser vendidos. De acuerdo a Symantec, el valor promedio que una tarjeta de crédito tiene en los mercados negros es de 100 dólares, 125 por una cuenta bancaria, 12 por una dirección de correo electrónico, 7 por un número de seguridad social, por nombrar algunos [11].

[16] Arquitectura de aplicaciones distribuidas que dividen tareas, cargas de trabajo y recursos entre los equipos miembro, sin necesidad de una coordinación central.

[17] Cualquier caso en el que un atacante busque convencer a la víctima de hacer algo que no debería. El objetivo es que cada intento de engaño no pueda, o sea muy difícil de diferenciar, de algo legítimo para el usuario.

- Typo-squatting. Un atacante registra nombres de dominio similares a los de entidades legítimas con la finalidad de que, cuando un usuario cometa un error al escribir la dirección web de un sitio (por ejemplo, www.bancoomer.com.mx en lugar de www.bancomer.com.mx), sea direccionado a una página maliciosa.

- Subdominios. Un atacante registra nombres de dominio similares a posibles subdominios con los que una entidad legítima podría contar (por ejemplo, banamex.online-banking.com como subdominio de banamex.com), con la finalidad de utilizar tales direcciones en un engaño por correo electrónico, debido a que es bastante complicado que un usuario note que no forman parte de su institución bancaria.

- Suplantación DNS (pharming.) En esta forma de suplantación, la víctima es direccionada a un sitio web fraudulento, que para el caso de la banca electrónica se trata de la réplica de algún portal financiero, alterando las respuestas DNS[18] que van hacia su equipo, ya sea mediante la instalación de código malicioso que modifique el archivo hosts[19] propio de su sistema operativo, que modifique las respuestas de su enrutador local o a través de un ataque de hombre en medio, mediante un punto de acceso inalámbrico, un servidor proxy[20] o un nodo TOR[21] maliciosos.

- Suplantación de voz (vishing.) En el pasado, este ataque consistía en llamadas telefónicas a un gran número de personas que, al responder sufrirían un intento de engaño a través de la ingeniería social para proveer información sensible. Actualmente este método se complementa con correos electrónicos: el mensaje fraudulento no contiene un enlace que direcciona a un sitio web malicioso, sino que tiene un número telefónico al que piden que la víctima se comunique. Al hacerlo, un sistema de banca telefónica automatizado, clonado por el atacante, atenderá la llamada y buscará obtener la información del usuario a través de sus menús interactivos.

- Redes sociales. Es actualmente un campo muy fértil para los atacantes. Millones de personas poseen una o más cuentas en redes sociales, muchas de ellas con poco o nulo cuidado de su información personal. Adicionalmente, y debido a que no existen restricciones respecto a quién puede registrarse, cualquier atacante puede confundirse entre los contactos de un usuario e intentar llevar a cabo cualquiera de los ataques a la banca electrónica mencionados en párrafos anteriores, a través de ingeniería social, suplantación, robo de identidad, infecciones a través de aplicaciones, correo no deseado, etc.

[18] Sistema distribuido y jerárquico para asociar nombres de dominio con direcciones IP a nivel mundial.
[19] Archivo usado por un sistema operativo para ligar nombres de dominio con direcciones IP.
[20] Servidor que actúa como un intermediario para las peticiones de clientes que buscan acceder a los recursos de otros servidores. La problemática radica en que no se puede tener la certeza de quién está administrándolo, por lo que cualquiera podría estar leyendo y modificando todo el tráfico no cifrado.
[21] The Onion Router. Técnica para obtener comunicación anónima en una red de computadoras. Los mensajes son repetidamente cifrados y enviados a través de computadoras voluntarias (llamados onion routers) que, como si de pelar una cebolla se tratara, "pelan" cada capa de cifrado para conocer las siguientes instrucciones de ruteo. Es imposible para cada nodo intermedio conocer el origen de los mensajes y el destino final, se limitan a descubrir el siguiente salto en la red de computadoras voluntarias.

### *2.1.1.3 Mirar sobre el hombro, registradores, hombre en medio*

Una técnica adicional para obtener credenciales de acceso se basa en "observar" mientras el usuario las ingresa. Lo anterior puede lograrse al tener el evento dentro de nuestro campo visual y mediante hardware o software especializado.

- Mirar sobre el hombro (shoulder surfing.) Consiste en "mirar sobre el hombro" del usuario cuando éste ingresa información de autenticación en un sistema. Tradicionalmente requiere presencia física y oportunismo por parte del atacante, sin embargo, cada vez es más frecuente la instalación de cámaras de circuito cerrado que observan y graban las contraseñas o PIN de los cuentahabientes.

- Registradores (loggers.) Son dispositivos o piezas de software que tienen la finalidad de registrar, para posterior análisis, las pulsaciones en un teclado (keyloggers) o las imágenes en pantalla al hacer clic en un ratón (mouselogger) dependiendo del registrador utilizado. En el contexto de la banca electrónica se encuentran orientados a la captura de las credenciales de acceso a los servicios de los cuentahabientes.

  Los registradores basados en software son considerados código malicioso e incluso varios caballos de Troya son capaces de implementar este tipo de funcionalidades para el atacante, sin embargo, existen igualmente registradores de teclas basados en hardware, los cuales son conectados entre el cable del teclado y el CPU, en una computadora personal.

- Hombre en medio. Se presenta cuando una entidad establece conexiones independientes con dos víctimas (un cliente y un servidor bancario), haciéndoles creer que están efectuando una comunicación directa a través de una conexión privada cuando de hecho toda la conversación es controlada y manipulada por el atacante. Este ataque puede ser realizado de forma pasiva, en donde únicamente se observa la información intercambiada, o activo, en donde además de interceptar la comunicación, ésta es modificada antes de direccionarla al destino.

  - Nodo TOR malicioso. A pesar de que en una red TOR todos los datos en tránsito están cifrados, la comunicación entre el penúltimo nodo y el destino viaja en claro a menos que un cifrado a nivel de aplicación sea utilizado. Siendo así, si tal nodo se encuentra comprometido, éste tiene la posibilidad de observar y/o modificar todo el tráfico que pasa a través de él (Figura 3.)

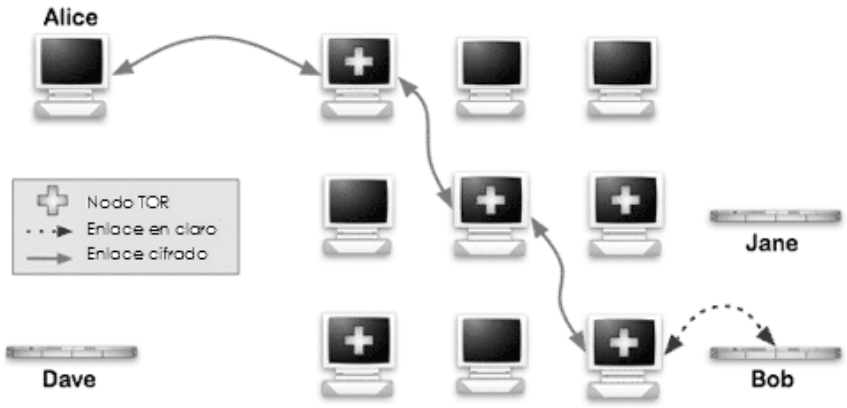


Figura 3. Enlaces en una red TOR[22].

- Punto de acceso malicioso. Cuando un usuario de laptop o dispositivos móviles se encuentra fuera del alcance de su red inalámbrica personal o corporativa, y no cuenta con acceso a internet provisto por algún comercio a sus clientes, opta generalmente por establecer una conexión con la primera red "libre" que encuentre y, si la comunicación es exitosa, no se preocupa más por el hecho.

  Con la tecnología existente en la actualidad, las tarjetas de red inalámbrica presentes en computadoras personales y otros dispositivos pueden ser configuradas para "compartir la red" y actuar como un punto de acceso. Por tanto, si la acción anterior es realizada por un atacante, éste puede interceptar y modificar todo el tráfico que fluye por el punto de acceso malicioso, es decir, su propia computadora.

- Servidor proxy malicioso. Existen servidores proxy públicos disponibles en la red que son utilizados generalmente para evadir restricciones de acceso locales o monitoreo. Estos servidores son identificados por sus usuarios a través de búsquedas y listas, con el inconveniente de que no existe ninguna regulación referente a su creación o a la persona que administra el servicio.

  Considerando lo anterior, el propietario de un servidor malicioso de este tipo puede interceptar toda comunicación que viaja a través del proxy y, si lo desea puede igualmente modificarla y redirigirla a voluntad.

- En redes locales. Aprovechando vulnerabilidades del protocolo ARP[23] (los equipos en una red local no tienen manera de autenticar el origen de las respuestas ARP y las asociación de direcciones que éstos mantienen en caché son sobreescritas cuando una nueva respuesta arriba, sin importar si las anteriores han expirado o no), un atacante puede asociar su dirección MAC con la dirección IP de un objetivo, provocando que todo tráfico destinado a la víctima sea enviado al atacante. Éste tiene la opción de analizarlo mediante

[22] Basada en la imagen "How Tor Works" de Tor Project, contenida en "Tor: Overview", consultada el 28 de Julio del 2013 en https://www.torproject.org/about/overview.html.en.

[23] El Protocolo de Resolución de Direcciones (ARP, por sus siglas en inglés), tiene la finalidad de asociar direcciones de capa de red (IP) con direcciones de capa de enlace (MAC.)

un monitoreo del tráfico y reenviarlo a su destino original, o modificar los datos adicionalmente.

Es evidente entonces que, si los usuarios capturados mediante alguna de las variaciones de hombre en medio descritas, buscan establecer contacto con sus servicios de banca electrónica mientras permanecen en estas conexiones apócrifas, toda su información queda a disposición del atacante.

### 2.1.2 Redes y servicios bancarios

Los esfuerzos de los atacantes en este sentido tienen que ver, en primer lugar, con la búsqueda de vulnerabilidades a nivel de aplicación o sistema operativo que les permitan ganar un cierto nivel de control sobre la infraestructura de las instituciones bancarias y, por tanto, sobre las transacciones que en ella se realizan. Sin embargo, la explotación de vulnerabilidades en este punto de control no se limita al compromiso de equipos o aplicaciones, sino que pueden estar enfocadas al cese completo de operaciones.

#### *2.1.2.1 Mal diseño de aplicaciones cliente-servidor*

El desarrollo de aplicaciones es cada vez más complejo. El incremento en el número de funcionalidades las hace de mayor tamaño, la gran variedad de dispositivos y de sistemas operativos a los que los usuarios tienen acceso las hacen en muchas ocasiones multiplataforma, la competencia y la demanda del mercado exigen su liberación en periodos de tiempo cada vez más cortos, lo que provoca que el producto final llegue a las manos de los consumidores con un gran número de vulnerabilidades de las que no se tiene conciencia y altamente susceptibles a ser atacadas.

Un ejemplo muy común de lo antes mencionado son los navegadores web. En 2011 fueron identificadas 500 vulnerabilidades en estas aplicaciones (191 en Chrome de Google, 119 en Safari de Apple, 100 en Firefox de Mozilla, 50 en Internet Explorer de Microsoft y 31 en Opera, de la compañía homónima), algunas de ellas bastante críticas [12]. Para intentar corregir las vulnerabilidades que van encontrándose, las compañías liberan parches de seguridad, sin embargo, la identificación de la falla específica significa que ésta ya ha sido explotada con anterioridad por cierto periodo de tiempo y que una gran cantidad de personas fueron afectadas por el pobre diseño de los proveedores.

En el caso de los servidores y aplicaciones web en el que muchas de las funcionalidades de la banca electrónica están basadas, existen un gran número de vulnerabilidades que año con año siguen sin ser atendidas por varias instituciones. OWASP[24], en su reporte anual 2013, señala las siguientes como algunas de las más frecuentes [13]:

- Inyección. Consiste en incluir sentencias propias de algún lenguaje de programación o de definición de datos dentro de un formulario, con la intención de provocar la ejecución de un comando por parte de una aplicación web. Lo anterior es posible cuando no se realiza correctamente un filtrado de los caracteres de ingreso, permitiendo así la formación de las instrucciones con fines maliciosos.

[24] Open Web Application Security Project. Es una comunidad que incluye corporaciones, organizaciones académicas e individuales de todo el mundo que crea artículos, metodologías, documentación y herramientas con la finalidad de concientizar acerca de la seguridad de las aplicaciones web.

La forma más común que este ataque presenta es la inyección SQL, cuyos comandos buscan obtener información de la base de datos que la aplicación web objetivo consulta, sin embargo, ataques que inyectan comandos dirigidos al sistema operativo que aloja a la aplicación también son posibles.

- Secuencia de comandos en sitios cruzados (cross site scripting.) Ocurre cuando un atacante utiliza una aplicación web para hacer llegar código malicioso, generalmente a través de la inyección de una secuencia de comandos (script) que se ejecuta del lado del navegador, a otro usuario. Esto es posible cuando la aplicación utiliza datos ingresados por los usuarios, sin una correcta validación o codificación, para generar sus respuestas. Existen dos tipos de variantes:

    - Persistente. El código de la secuencia de comandos se encuentra permanentemente alojado en el servidor vulnerable, de tal manera que cuando otro usuario realiza una petición, los datos almacenados son incluidos en la respuesta de la aplicación que, al ser procesada por el navegador del cliente, ejecuta la secuencia de comandos maliciosa.

    - Reflejada. El código de la secuencia de comandos es recuperada desde una ubicación diferente, desde la cual es enviada al servidor vulnerable una vez que el usuario hace clic en una URL maliciosa. Una vez recibida, el servidor utiliza estos datos de entrada para crear la respuesta de la aplicación que, al ser procesada por el navegador del cliente, ejecuta la secuencia de comandos maliciosa.

- Falsificación de peticiones en sitios cruzados (cross site request forgery.) Está enfocada a engañar a un usuario para que realice acciones no deseadas en una aplicación web en la que ya se encuentra autenticado. Esta acción puede ser lograda al provocar la carga de una dirección que contiene una petición falsa, la cual hereda la identidad y privilegios de la víctima debido a que los navegadores, para la mayoría de los sitios existentes, adjuntan automáticamente las credenciales asociadas a éste (vía galletas HTTP, contraseñas almacenadas, etc.) con cada petición, por lo que el servidor destino no tiene manera de discriminar las peticiones falsas de las auténticas.

- Referencias inseguras y directas a objetos (insecure direct object references.) Se suscita cuando un desarrollador expone una referencia a un objeto interno de la aplicación, el cual puede ser un archivo, una carpeta, una llave de base de datos, una URL, etc. Si no se cuenta con las medidas de control de acceso adecuadas, un atacante puede identificar alguna de estas referencias e intentar modificarlas para obtener acceso a objetos restringidos de manera no autorizada.

#### *2.1.2.2 Denegación de servicio*

Cualquier acción que afecte la disponibilidad de los recursos bancarios en línea y, por tanto, impida al usuario realizar transacciones legítimas es una denegación de servicio.

Comúnmente este ataque es llevado a cabo realizando tal número de peticiones a los servidores que sobrepasan la capacidad que éstos tienen para atenderlas. Los resultados de este tipo de acciones van desde provocar lentitud en los servicios hasta colapsarlos completamente. A pesar de que no involucra destrucción de información ni acceso no autorizado a zonas restringidas, la denegación de servicio es altamente perjudicial para

cualquier institución debido a que impide la utilización de los servicios por parte de los usuarios que, en última instancia, tiene como consecuencia pérdida de dinero y de reputación.

En los últimos tiempos, la razón cada vez más común por la que se busca colapsar los servicios de alguna institución es el hacktivismo[25], que se basa en la denegación de servicio distribuida[26] a través de la planificación de ciertos colectivos o vía redes de bots.

#### *2.1.2.3 Ataques internos*

Cuando se piensa en ataques a los sistemas, la percepción general es que el responsable es un atacante externo, sin embargo, la gran mayoría de las veces las amenazas más grandes provienen del interior. En 2011, los ataques internos fueron el cuarto tipo de ataque más frecuente al que se enfrentaron las empresas [14].

Los empleados, que tienen acceso a información privilegiada, tienen la posibilidad de explorar los sistemas a voluntad sin dejar huella cuando los procesos internos de seguridad no son lo suficientemente buenos y, como consecuencia, los robos por parte de trabajadores son más frecuentes que los realizados por ladrones externos. Por otro lado, aunque el personal no tenga intenciones maliciosas, sus acciones pueden derivar en la exposición de información sensible, de manera no intencionada, que puede ser explotada por otros.

### 2.1.3 Canales de comunicación

En una transacción electrónica es esencial un medio seguro, siendo éste aquel en el que el usuario tiene la certeza de que la comunicación está siendo realizada con su institución financiera y que además la información intercambiada, que es de alta criticidad, no pierde su confidencialidad.

Existen varios protocolos que, en conjunto, logran establecer este tipo de canales de comunicación considerados seguros y, como se explicará posteriormente, las instituciones financieras estructuran de manera similar sus medidas de seguridad en este respecto. Siendo así, los esfuerzos de los atacantes en este punto de control están más dirigidos a alterar o impedir el establecimiento de los canales de comunicación seguros que a atacarlos una vez que están plenamente estructurados.

Para lograr lo anterior, puede ser utilizada alguna de las variantes de hombre en medio antes descritas buscando que el canal se establezca entre el usuario y el atacante, quien posteriormente puede modificar y direccionar los datos o transacciones a la institución legítima. Adicionalmente, el compromiso del equipo del cuentahabiente mediante la instalación de algún tipo de código malicioso hace innecesario el intentar vulnerar el canal de comunicación, ya que los datos y transacciones podrían ser alterados desde el origen.

[25] Es el uso de computadoras y redes de computadoras para promover la protesta, el activismo y la desobediencia civil.
[26] Múltiples equipos son utilizados para atacar un único objetivo, provocándole denegación de servicio.

## 2.2 Medidas de seguridad

En virtud de la gran cantidad de amenazas a las que se encuentran expuestos los sistemas, medidas de seguridad adecuadas son necesarias para mitigar riesgos y los costos asociados a ellos. En muchos casos se establece un balance entre la inversión que se realiza en temas de seguridad y el costo potencial de la explotación de riesgos residuales y, adicionalmente, se busca reducir lo más posible el costo del lado del cliente para que éste pueda utilizar los servicios electrónicos con la infraestructura con la que ya cuenta. La banca electrónica no es una excepción, sin embargo, aunque esta flexibilidad hace a los servicios más atractivos, tiene un impacto en la seguridad, debido a que en la práctica los bancos establecen el mínimo de seguridad necesario para cubrir la mayoría de los riesgos, priorizando al máximo la funcionalidad y la conveniencia [7].

Dentro de las medidas de seguridad hay dos aproximaciones que deben cubrirse y que se complementan entre sí, los controles tecnológicos y los controles regulatorios.

### 2.2.1 Controles tecnológicos

Considerando los puntos de control establecidos, así como las posibles maneras de vulnerarlos, saltan a la vista cuatro frentes principales en los que las medidas de protección se enfocan: seguridad en las comunicaciones, autenticación de entidades y transacciones, protección de redes y servicios bancarios y medidas anti-suplantación.

#### *2.2.1.1 Seguridad en las comunicaciones*

Todos los datos entre cliente y banco viajan a través de internet, lo que implica el flujo entre cientos de enrutadores y servidores. El establecimiento de un canal de comunicación seguro en el que se pueda proteger la confidencialidad y verificar exitosamente la integridad de la información es imperativo, tomando en cuenta la potencial criticidad de las transacciones que se realizan a través de los servicios financieros.

Una de las maneras más utilizadas para lograr lo anterior es mediante el uso de los protocolos SSL/TLS[27].

SSL/TLS

Son protocolos criptográficos que proveen un canal seguro entre cliente y banco, mediante el establecimiento de confidencialidad a través de criptografía simétrica[28], de verificación de integridad a través de MACs[29] y mediante el uso de criptografía

[27] Secure Sockets Layer/Transport Layer Security. TLS es el sucesor de SSL, sin embargo, casi la totalidad de sitios web y navegadores soportan tanto la última de versión de SSL (3.0), como la primera versión de TLS (1.0), que son compatibles entre sí.

[28] Los algoritmos de llave simétrica utilizan la misma llave tanto para cifrar como para descifrar un mensaje. Su principal problema es la distribución de esta llave compartida entre las partes que se quieren comunicar, ya que al viajar por la red es susceptible de ser interceptada por terceros.

[29] Message Authentication Code. Pieza de información utilizada para verificar la autenticidad e integridad de un mensaje. El algoritmo que lo genera tiene como entrada una llave secreta y un mensaje de longitud variable, produciendo un código único e irrepetible para el mensaje procesado. Si el mensaje es alterado, el código resultante igualmente variará significativamente.

asimétrica[30] para acuerdo de llaves de cifrado. Debido a que no se aplica ningún tipo de firma digital[31] en los datos del emisor, estos protocolos no facilitan el no repudio de transacciones en la sesión segura por sí mismos.

Tras una solicitud directa del cliente para establecer una conexión segura, toma lugar el siguiente proceso:

1. Cliente y servidor se envían información para establecer conjuntamente los parámetros que se utilizarán en la conexión, como la versión del protocolo (por razones de compatibilidad), algoritmos de cifrado disponibles (se elige el más fuerte que tengan en común), entre otra.

2. El servidor envía su certificado digital[32] para poder ser autenticado por el cliente. De igual manera, si el cliente solicita acceso a algún recurso que requiere autenticación, se le requerirá a éste su propio certificado, aunque en la práctica sucede con muy poca frecuencia.

3. Con la información recibida hasta el momento, el cliente genera una llave de sesión que compartirá con el servidor, a quien se la hará llegar cifrada con su llave pública, incluida en el certificado del punto anterior.

4. Una vez que ambos lados de la comunicación cuentan con la llave de cifrado que utilizarán en la conexión, se informan mutuamente que todo futuro mensaje será cifrado con ésta.

Una vez establecida la conexión, todo dato transmitido por ambas partes será dividido en fragmentos, cada uno de los cuales tendrá asociado un MAC y, ambos cifrados, serán enviados en conjunto.

SSL/TLS puede ejecutarse desde un navegador web (utilizando la modalidad de banca por internet) o a través de una aplicación dedicada o un applet (utilizando la modalidad de banca en casa). En cualquier caso, la seguridad de este protocolo depende en gran medida de una infraestructura confiable que garantice las ligas entre llaves públicas e instituciones (en este caso bancos) a través de certificados, que son expedidos y respaldados por autoridades certificadoras.

Al recibir el certificado de un banco, el cliente verifica en primera instancia su autenticidad a través de la existencia de la firma de la autoridad certificadora que lo expidió, que a su vez es validada mediante certificados raíz que se incluyen generalmente en la instalación de los sistemas operativos y navegadores web, para las autoridades más

[30] Los algoritmos de llave asimétrica utilizan dos llaves separadas ligadas matemáticamente, una pública y una privada. Una de ellas es utilizada para cifrar un mensaje y la otra para descifrarlo. Bajo la premisa de que una de las llaves se mantiene en secreto, el cifrar un mensaje con una llave pública garantiza que sólo el poseedor de la llave privada puede descifrarlo. Por el contrario, un mensaje cifrado con una llave privada, a pesar de poder ser descifrado por todo aquel que conozca la llave pública, garantiza que sólo el poseedor de la llave privada pudo haberlo cifrado, hecho que justifica de manera simplificada a las firmas digitales. Adicionalmente, estos algoritmos pueden ser utilizados para acordar llaves simétricas entre dos entidades.

[31] Esquema matemático para demostrar la autenticidad de un documento electrónico. Una firma digital válida le da al receptor la seguridad de que el documento fue realmente creado por el emisor, de que éste no puede negar su envío y que el mensaje no fue alterado en su camino.

[32] Documento electrónico que utiliza una firma digital para ligar una llave pública con una entidad.

conocidas y/o confiables. Cuando alguna de las varias validaciones no prospera, entonces el navegador o la aplicación notificarán al usuario y pedirán su confirmación para continuar o terminar con la conexión.

Los entornos inalámbricos utilizan una adaptación de TLS, llamada WTLS, para dispositivos pequeños con limitaciones de ancho de banda, memoria o procesamiento. Basa su optimización en la utilización de criptografía de curvas elípticas[33] y en la definición de su propio formato de certificado digital, aunque también acepta el estándar utilizado por SSL/TLS.

La obtención de un certificado implica una importante cantidad de dinero, por lo que varias compañías optan por crear los propios para utilizarlos en sus servicios web, sin embargo, al no poder ser verificarlos con ninguna autoridad, los navegadores notifican la posibilidad de encontrarse en un sitio ilegítimo aunque los servicios sean auténticos. Debido a lo anterior, las instituciones piden de antemano en algunas ocasiones el ignorar tales advertencias e ingresar a sus sitos que, si bien no causa daño alguno en esa ocasión específica, predispone al usuario a realizar lo mismo en posteriores oportunidades, con sitios potencialmente maliciosos, debido a que no cuentan con la información necesaria para tomar una decisión de seguridad correcta.

Más aún, un atacante puede seguir el proceso de obtención de un certificado digital para su sitio fraudulento y, en ese caso, los navegadores no realizarán advertencia alguna.

Cuando se habla de establecer un canal de comunicación seguro entre un cliente y un banco se asume que la computadora del usuario, su sistema operativo y sus aplicaciones son seguros, pero desafortunadamente éste no es el caso en la mayoría de las ocasiones. Estas plataformas son muy vulnerables a todo tipo de código malicioso que puede cambiar los certificados raíz instalados, robar llaves privadas y, en general, interceptar los datos de la comunicación antes de que ésta se asegure con los protocolos SSL/TLS, lo cual es un problema adicional que debe resolverse.

### *2.2.1.2 Autenticación*

Las medidas de protección en este sentido no sólo contemplan la autenticación del usuario ante el banco para acceder a los servicios, sino que además buscan corroborar la validez de cada una de las transacciones que los usuarios realicen dentro de las sesiones.

#### 2.2.1.2.1 Factor de autenticación único

La autenticación de un solo factor se refiere generalmente al uso de contraseñas fijas, las cuales pueden tratarse de un PIN o de una cadena de caracteres alfanuméricos que se combina con un número de cuenta para el servicio. En algunas ocasiones, el banco puede solicitar un subconjunto de los números o caracteres que conforman la contraseña, con la finalidad de proveer un cierto grado de seguridad antes ataques de monitoreo de tráfico y "mirar sobre el hombro". A pesar de los tan conocidos riesgos inherentes de este mecanismo (además de encontrarse expuesto a la aplicación de la ingeniería social, es vulnerable a ataques de diccionario y fuerza bruta), su utilización es aún muy amplia

[33] Aproximación a la criptografía de llave pública basada en la estructura algebraica "curva elíptica", definida sobre campos finitos. Su diseño hace posible alcanzar niveles de seguridad similares a los de otros algoritmos de cifrado, utilizando llaves más pequeñas.

debido a su facilidad de implementación y uso, sin embargo, se limita a la autenticación de entidades y no de transacciones.

Una manera de proveer un mayor nivel de seguridad en el uso de este tipo de contraseñas es a través del despliegue de un teclado virtual en la pantalla de la computadora del usuario, que es utilizado para ingresar datos de autenticación (mediante clics) cuando son requeridos. Estas aplicaciones protegen únicamente contra el monitoreo a base de registradores de teclas, debido a que tanto caballos de Troya como registradores de ratón tienen la posibilidad de impresiones de pantalla del teclado virtual en el momento en que es utilizado.

#### 2.2.1.2.2 Factor de autenticación múltiple y autenticación fuera de banda

Esta modalidad requiere la presentación de dos o más factores de autenticación, siendo éstos "algo que el usuario sabe", "algo que el usuario posee" o "algo que el usuario es."

Entre los mecanismos utilizados en la banca electrónica, pertenecientes al factor de posesión, se encuentran los siguientes:

- Contraseñas dinámicas. Son contraseñas de un solo uso. En ciertos casos las instituciones bancarias proveen al usuario con un listado de contraseñas que, una vez utilizadas, dejan de ser válidas. Tanto cliente como servidor deben mantener sincronización en cuanto a cuáles contraseñas ya han sido ingresadas y cuál es la próxima. Este mecanismo tiene la desventaja de que el usuario difícilmente recordará la totalidad de contraseñas y su validez, por lo que generalmente las mantienen en papel o archivos electrónicos, lo que las hace susceptibles a ser conocidas por terceros.

  Es común que se utilicen combinaciones de los dos últimos puntos: contraseñas fijas para la autenticación de entidades y contraseñas dinámicas para la autenticación de transacciones.

- Esquema reto/respuesta. Esta forma de autenticarse no hace uso de una contraseña, sino de la respuesta a un reto aleatorio generado por el servidor que involucra un secreto compartido. Un ejemplo de lo anterior son las llamadas "tablas aleatorias de contraseñas": el reto consiste en la selección por parte del servidor de una posición dentro de la tabla compartida (una relación renglón – columna dentro de una cuadrícula) y la respuesta serían la contraseña asignada en tal posición.

  La penetración de los dispositivos móviles ha permitido la modificación de este esquema en la forma de reto SMS, el cual consiste simplemente en el envío de un mensaje de texto por parte del banco al teléfono del cuentahabiente, el cual contiene un código de confirmación que el usuario utiliza para autenticarse.

- Generadores de contraseñas dinámicas (tokens.) Los mecanismos antes mencionados pueden ser implementados de manera más segura a través de generadores, que son piezas de hardware o software utilizadas como un segundo factor de autenticación, pretendiendo ser "algo que el usuario posee", a través de contraseñas de un solo uso generadas por el dispositivo o aplicación.

Existen varios tipos de generadores: los basados en tiempo, los basados en evento y los basados en reto.

- Basados en tiempo. Existe una clave compartida entre banco y cliente, la cual se utiliza para generar cada contraseña de un solo uso. Cada código es el resultado del hash[34] de la hora del dispositivo concatenada con la clave compartida [15, p. 40] y, debido a que el banco necesita realizar el mismo procedimiento para hacerlos válidos, es necesaria la sincronización entre el generador y el servidor.

- Basados en evento. Esta clase de generadores crean códigos de un solo uso cada vez que un evento específico, que puede consistir en presionar un botón del dispositivo o ingresar un PIN en el mismo, se realice. Son asíncronos y los códigos generalmente son resultado de hash concatenados (diplomado), es decir, la contraseña n = hash(contraseña n-1.) Del lado del servidor, los códigos se validan verificando que a partir de la última contraseña utilizada se pueda llegar a la que se está intentando validar.

- Basados en reto. El servidor hace llegar un reto en forma de número que debe ser ingresado en el generador, que lo procesa y responde con una confirmación a través de la cual el usuario se autentica.

Además de los generadores con hardware dedicado, existen aquellos en forma de software alojado en dispositivos electrónicos como computadoras, laptops, tabletas o teléfonos inteligentes. Conservan las características y tipos de sus contrapartes físicas, sin embargo se encuentran expuestos a riesgos adicionales como código malicioso o vulnerabilidades en el diseño de las aplicaciones. Los hay también con conexión USB, utilizados generalmente en las aplicaciones de banca en línea, las cuales se comunican directamente con el dispositivo cuando lo requieren, sin necesidad de interacción con el usuario, salvo para colocar el hardware en el puerto correspondiente.

A pesar de que la función primordial de este mecanismo es la de autenticar identidad, algunos son capaces de generar MACs que pueden ser utilizados para autenticar transacciones.

Este segundo factor de autenticación representa una gran ventaja, pero existe un período de tiempo, que varía de acuerdo al tipo de generador utilizado, en que la contraseña de un solo uso puede ser utilizada por algún atacante si es comprometida, aunque tal problemática es atendida no permitiendo conexiones simultáneas. En última instancia, el dispositivo puede ser extraviado o robado, dejando a un agresor en posibilidad de generar los códigos que sean necesarios para sus fines.

Un sistema de autenticación requiere un registro de usuarios previo y la realización de acciones iniciales para configurar la cuenta de cada cliente, al cual se le entrega una contraseña inicial en papel o por algún otro medio inseguro. Si esta contraseña es

[34] Una función hash es un algoritmo que mapea segmentos de datos de una longitud variable a una cadena de caracteres de longitud física, llamada hash. Un valor hash puede ser utilizado para verificar la integridad de un archivo, debido a que una mínima modificación en el mismo produciría un valor hash completamente diferente.

obtenida antes de se haya modificado en el sistema o, en general, si el dispositivo utilizado se encuentra comprometido por algún tipo de código malicioso, el resto de los mecanismos de autenticación quedan inservibles. Debido a lo anterior, de manera complementaria a la utilización de factores de autenticación adicionales, se recomienda que éstos sean intercambiados a través de redes o canales diferentes a aquél donde las transacciones están siendo realizadas, bajo la premisa de que vulnerar dos medios de transmisión independientes entre sí es más complicado y menos probable. Esta interacción se denomina autenticación fuera de banda.

Otro problema adicional es el de la delegación, en el que el titular de las cuentas desea compartir el acceso con alguna persona, por ejemplo, un subordinado. Si los métodos de autenticación no permiten diferenciar al subordinado del titular, entonces no hay delegación, sino suplantación de identidad. En este tipo de casos, el sistema debe permitir la creación de cuentas secundarias con acceso y privilegios limitados.

#### *2.2.1.3 Protección de redes y servicios bancarios*

Tras resguardar las comunicaciones lo mejor posible, el siguiente conjunto de controles busca la protección de las redes y sus servidores, así como la de los clientes que acceden a ellas. Una manera de lograr lo anterior es a través del control de acceso a la red (NAC, por sus siglas en inglés), que es una metodología formal para identificar, controlar y asegurar los accesos a recursos y servicios críticos, tomando en cuenta perfiles de usuario o dispositivo, hora, geografía, estado de salud del equipo suplicante, entre otros.

Esta aproximación considera, de manera general, los puntos siguientes [16]:

- Detección y autenticación. El primer paso consiste en identificar quién está intentando conectarse a la red y desde dónde, permitiendo una reacción dinámica y automática por parte de la infraestructura, en base a las reglas establecidas para el dispositivo o usuario detectado.

  Identificación y autenticación van de la mano y, en general, el mecanismo implementado para autenticar es igualmente utilizado para identificar. Una arquitectura NAC puede soportar varios métodos para la realización de estas actividades, de acuerdo a las necesidades de cada entidad.

  - Basada en IEEE 802.1X. Involucra a un suplicante que provee sus credenciales a un dispositivo autenticador (un conmutador o un punto de acceso inalámbrico), quien a su vez las reenvía a un servidor de autenticación (un equipo con RADIUS[35] instalado), quien determina la validez de las credenciales y permite/deniega el acceso a la red. Inicialmente, este estándar permite únicamente el tipo de tráfico necesario para intercambiar datos de autenticación, a través del puerto al que el dispositivo suplicante se encuentra conectado. Cuando el servidor de autenticación así lo determina, se otorgan acceso y permisos de acuerdo al perfil del usuario o del equipo.

    Este método es capaz de autenticar tanto a usuario como a equipo, ya sea de manera individual o como entidad conjunta, sin embargo, hay

[35] Remote Authentication Dial In User Service. Protocolo que provee administración centralizada de la autenticación y autorización de dispositivos que se conectan y usan un servicio de red.

ocasiones en que, debido a que algunos dispositivos (como conmutadores, impresoras o cámaras IP antiguos) no soportan o no contienen un suplicante 802.1X, no resulta la manera de autenticar más adecuada.

- Basada en MAC. Utiliza los mismos componentes básicos que 802.1X, con la diferencia de que el conmutador reemplaza las credenciales de usuario por la dirección MAC del equipo que desea acceder a la red, la cual verifica con el servidor RADIUS. Si se utiliza como complemento a 802.1X, se logra la autenticación de usuario y dispositivo mencionada anteriormente.

  Ofrece un nivel de seguridad limitado, ya que autorizaciones posteriores quedarán ligadas al hardware únicamente, sin importar quién esté en posesión del mismo.

- Basada en Web. Este método de autenticación redirecciona todo intento de conexión hacia un portal web, donde el usuario debe proveer sus credenciales. Una vez que la autenticación es exitosa, la utilización de los servicios asociados al perfil del usuario o equipo es permitida.

- Evaluación. Cuando un usuario es autenticado de manera exitosa, es enviado inicialmente a una red privada de cuarentena, donde se evalúa el estado de salud de su equipo para verificar su cumplimiento con los requisitos de seguridad mínimos establecidos por la red. Determinar el método adecuado para tal evaluación depende principalmente de lo que se busque comprobar y las opciones que los dispositivos soporten.

  - A través de un agente. Se trata de una pieza de software que corre en el dispositivo y que provee información acerca del estado del cortafuegos, el antivirus y la actualización de sus firmas, el sistema operativo y sus actualizaciones, el software adicional instalado y los procesos y servicios en ejecución, entre otros.

    Este agente puede ser cargado temporalmente o removido en cada evaluación (agente ligero), o puede encontrarse instalado de manera permanente, junto con algún cortafuegos o detector de intrusiones, en el dispositivo (agente pesado.)

  - Sin agente. Puede realizarse remotamente a través de un escáner en red, en cuyo caso se analizan puertos abiertos, servicios que corren, vulnerabilidades asociadas a servicios o versiones específicas, etc.

    Una manera adicional es mediante un applet, vía un navegador web, que inicie funciones de evaluación de manera local, reportando los resultados al administrador.

Es de suma importancia mantener al día las actualizaciones de seguridad que los diferentes proveedores suministran a sus sistemas operativos y aplicaciones, para evitar que un atacante tome ventaja de alguna vulnerabilidad que le permita ganar acceso a los equipos y, en última instancia, a la red.

Adicionalmente, la instalación de software antivirus permite identificar y eliminar los tipos de código malicioso más comunes, tanto los que pretenden ingresar a los sistemas, como aquellos ya residentes en ellos, si es el caso. Algunas aplicaciones

de este tipo cuentan con funcionalidades avanzadas, como el análisis de correos electrónicos (con la intención de filtrar aquellos que pudieran ser fraudulentos), un cortafuegos personal y hasta la detección y supresión de bots [6, p. 307].

En la mayoría de ocasiones, tanto sistemas operativos como aplicaciones cuentan igualmente con mecanismos nativos que, correctamente configurados, proveen capas de seguridad adicionales sin necesidad de tecnologías complementarias, proceso que se conoce como "hardening"[36].

- Autorización/Contención. Una vez que un dispositivo fue detectado, autenticado y evaluado con resultados positivos, el acceso a la red y a servicios específicos es concedido al usuario.

  La manera más común de realizar lo anterior es mediante el uso de VLANs dinámicas, con la finalidad de separar los dispositivos no autenticados y no evaluados de las redes de producción.

  Cuando un equipo correctamente autenticado no cumple con los requisitos mínimos de seguridad en la fase de evaluación, permanece en la red de cuarentena hasta que sus problemas sean resueltos, con la menor interacción posible tanto de usuarios como de administradores, en una fase de remediación provista por la propia arquitectura NAC.

- Remediación. Una remediación completamente automática requiere la presencia de un agente que pueda realizar cambios en configuraciones e instalación de servicios faltantes. En muchas ocasiones es utilizada alguna solución de administración de software como complemento a la arquitectura NAC, para realizar esta labor.

  Otra solución, que pone la responsabilidad en el usuario, es la redirección de la conexión hacia un "servidor de remediación", en donde a través de un portal web se muestran de manera explícita los requisitos de seguridad no aprobados por el equipo, la manera de solucionarlos, enlaces de descarga de software faltante y un enlace para reintentar la conexión.

  Una vez finalizada la remediación se inicia un nuevo proceso de evaluación, tras el cual se determina si se concede el acceso a la red y sus servicios o si es necesaria remediación adicional.

- Monitoreo. Aún cuando un dispositivo ha sido admitido en la red, es necesaria una evaluación post-conexión a intervalos regulares para asegurar que el equipo mantiene el cumplimiento de los requisitos mínimos de seguridad. Cuando una anomalía es detectada, nuevos procesos de evaluación y remediación son necesarios.

En el contexto de la banca electrónica, un primer control tomado de las metodologías NAC es la separación de redes internas de aquellos segmentos expuestos al público,

[36] Proceso para aumentar la seguridad en un sistema mediante de la reducción de su superficie de ataque, lo que cual es llevado a cabo generalmente a través de la remoción de software, cuentas o servicios innecesarios, entre otros.

contenidos en una zona desmilitarizada[37]. El primer elemento en esta infraestructura, que está enfocada a los usuarios que acceden a los servicios a través de un navegar web, es un cortafuegos. Este mecanismo, que puede ser una pieza de hardware o de software, filtra los paquetes que discurren por él (basarse en direcciones IP, números de puerto, tipos de servicio, entre otros), permitiendo o denegando el acceso a los flujos de datos entrantes (peticiones de clientes) o salientes (respuestas del servidor), de acuerdo a una política de seguridad establecida. Lamentablemente, si ésta no se encuentra correctamente diseñada o existen errores al reflejarla en las reglas de filtrado, la presencia de un cortafuegos no es garantía de seguridad.

Tecnologías adicionales dedicadas a la seguridad perimetral incluyen a los sistemas de detección (IDS)/prevención (IPS) de intrusos, cuya función es la de identificar o mitigar tanto intrusiones como extrusiones, a través de análisis de tráfico de red en busca de actividad anormal. La principal diferencia entre los dos sistemas mencionados es que el destinado a la detección opera fuera de línea, por lo que únicamente alerta en retrospectiva, mientras que el destinado a la prevención no sólo alerta en tiempo real, sino que busca mitigar los efectos de la actividad sospechosa detectada. El nivel de seguridad provisto por este tipo de dispositivos depende significativamente de un balance adecuado entre falsos positivos y falsos negativos, con el que todo juicio sobre las actividades analizadas es correctamente establecido.

Una petición legítima a la que los dispositivos de frontera hayan permitido el acceso se encontrará con una aplicación web de la institución financiera que, como primer medida de seguridad, se encuentra alojada en un sistema que no cuenta con los datos de los usuarios de manera local, por lo que accede a los sistemas bancarios que los contienen de manera remota [4]. Adicionalmente, y debido a que muchas aplicaciones de este tipo presentan frecuentemente vulnerabilidades en código, es de gran importancia la validación del mismo (ya sea por personal local o externo) para asegurar el correcto manejo de información de entrada y permisos de acceso, reduciendo así en gran medida la posibilidad de un ataque de inyección o de falsificación de peticiones.

Del lado de las terminales de trabajo y servidores de las instituciones financieras, así como de los dispositivos de los usuarios que cuentan con el servicio de banca en casa, la aplicación íntegra de una metodología NAC es imprescindible, debido a que un equipo comprometido puede poner en riesgo la red entera.

De igual manera, una práctica habitual dentro de las instituciones bancarias es la ejecución de revisiones periódicas a sus aplicaciones, sin importar si éstas se encuentran expuestas al público u operan de manera interna, tanto por sus propias áreas de seguridad informática como por auditores externos. Aunque el alcance de tales revisiones es diverso (por ejemplo, validar cumplimiento con leyes, regulaciones, estándares o políticas corporativas), la mayoría de ellas incluye revisiones a código fuente y pruebas de intrusión para la perspectiva técnica.

Finalmente, es de vital importancia la protección de los servicios financieros ante ataques que busquen evitar que se mantengan en funcionamiento, una de las amenazas de gran frecuencia y popularidad en la actualidad. Sin duda, la mitigación de ataques de

[37] Subred física o lógica que contiene y expone los servicios de una organización a una red más grande y no confiable, como internet. Su propósito es que un atacante sólo tenga acceso a los equipos en esta zona, proveyendo una capa de seguridad adicional a la red local de la organización.

denegación de servicio es una tarea ardua y que requiere de la participación de varios factores y entidades.

Una institución puede decidir no hacer nada y aceptar el riesgo de una denegación, puede compartir el riesgo a través de un seguro que absorba parte del impacto financiero o puede reducir el riesgo implementando alguna solución adicional a las empleadas tradicionalmente en el perímetro. Entre las más populares se encuentran los servicios "clean pipe"[38], el aprovisionamiento de ancho de banda excedente en un 75% al necesario para operar un sitio [17], la configuración de enrutadores de frontera para descartar todo paquete cuyo origen sea una dirección IP privada, instalación de dispositivos perimetrales con la funcionalidad de detección y bloqueo de ataques no volumétricos, redundancia en los centros de datos y, en los últimos tiempos, el filtrado de tráfico en la nube (un servicio provisto por terceros) antes de que éste llegue al sitio web.

Lamentablemente, ninguna de las soluciones anteriores es 100% efectiva, por lo que además de la implementación de controles es muy importante incluir los ataques de denegación de servicio como parte de los planes de continuidad y recuperación de desastres de las instituciones.

Debido a que la seguridad perfecta es imposible de alcanzar, de manera adicional a los mecanismos de protección descritos, las instituciones financieras deben realizar monitoreo constante y mantener bitácoras que permitan estudiar lo sucedido si una eventualidad se presenta, así como para disparar alertas si una transacción no va de acuerdo al perfil normal de algún cliente.

#### *2.2.1.4 Medidas Anti-suplantación*

En múltiples ocasiones se ha podido comprobar que el punto más vulnerable en un sistema son los propios usuarios que lo utilizan. A pesar del avance en este sentido, debido principalmente a la gran importancia que se le ha dado en los últimos tiempos a la educación y concientización de las personas, la suplantación es aún uno de los medios más utilizados para atacar los sistemas de banca electrónica, por lo que existen varios mecanismos de mitigación ideados para ayudar a los usuarios a tomar mejores decisiones.

- Filtros de correo no deseado. Uno de los medios de ataque por suplantación más comunes es a través de correos electrónicos con ligas a sitios web fraudulentos, por lo que todos los proveedores de este tipo de servicio trabajan de manera constante para establecer filtros que identifiquen los contenidos sospechosos. Su funcionamiento consiste en el análisis de características de los correos y en la asignación de un valor en base a ellas. Si dicho valor supera un límite preestablecido, el correo se etiqueta como no deseado. Adicionalmente, se establecen listas negras de remitentes identificados como distribuidores de correo no deseado [15, p. 29]. Una manera muy sencilla de evitar estos controles consiste en cambiar la fuente emisora de correos de manera constante, por ejemplo, distribuyendo los envíos entre los miembros de una red de bots.

- Anti-suplantación en navegadores web. De manera similar a los filtros de correo no deseado, los mecanismos nativos en navegadores realizan un análisis heurístico del contenido y metadatos de los sitios que, en conjunto con la información contenida

[38] En este tipo de servicios, el proveedor de servicios de internet se compromete, a través de un acuerdo de nivel de servicio, a brindar un cierto ancho de banda de tráfico legítimo y no sólo de tráfico total.

en servidores (listas negras en su mayoría), permite la clasificación de páginas web. Cuando un sitio se clasifica como "no seguro" el navegador actuará notificando el peligro al usuario, pidiendo confirmación para ingresar o bloqueando del todo a la página, cuya dirección es añadida a las listas negras del proveedor correspondiente. Desafortunadamente, estos análisis heurísticos no son 100% efectivos y presentan falsos positivos/negativos, además de que la actualización de listas negras no es inmediata, por lo que existe una ventana de tiempo en la que los usuarios pueden seguir siendo engañados a pesar de que la amenaza ya ha sido detectada.

- Software de terceros. Compañías especializadas ofrecen mecanismos de seguridad adicionales en forma de complementos o barras de tareas para navegadores web. Cada uno de ellos cuentan con funcionalidades diferentes y diversos grados de efectividad, sin embargo, en conjunto proveen las medidas siguientes de forma general:

    - Detección y notificación de sitios fraudulentos a través de análisis heurístico, asignación de valores, comparación con límites preestablecidos y listas negras que se actualizan con reportes de usuarios.

    - Prevención de envío POST[39] de la información de un formulario a un sitio web, cuando un usuario ha ignorado las advertencias de la aplicación anti-suplantación.

    - Capacidad de detectar si las credenciales del usuario han sido ingresadas en otro sitio diferente al de la sesión actual.

    - Ofrecer una mayor visibilidad de los protocolos TLS/SSL al usuario, permitiendo que éste no sólo observe las indicaciones características de una conexión segura en un navegador web (el candado o el cambio a HTTPS en la URL), sino que se muestra los detalles del certificado digital, así como de la autoridad certificadora que lo expide.

    - Capacidad de ligar marcadores[40] con el hash del certificado del sitio correspondiente. Si en algún momento la dirección de una página redirige a un sitio que no es el legítimo, el hash del nuevo certificado fraudulento no será el mismo que el almacenado, por lo que se notificará del peligro al usuario.

Otros controles utilizados para mitigar la suplantación son los ya mencionados sistemas multifactor y contraseñas de un solo uso enviadas fuera de banda, sin embargo, muchos de los ataques ya contemplan la solicitud y robo de estas contraseñas dinámicas.

Además de las medidas en equipos locales y servidores, existen grupos y asociaciones que se encargan de monitorear sitios web y de correo electrónico en busca de posibles intentos de suplantación. Cuando alguno es detectado, notifican al proveedor de servicios o al dueño de la página para que éste se encargue de su eliminación. Desafortunadamente, en el período comprendido entre la liberación del intento de suplantación, detección, notificación y remoción, un gran número de víctimas puede ser

[39] Método HTML diseñado para solicitar a un sitio web la recepción de datos encapsulados en el cuerpo de la petición. Es utilizado en el envío de formularios.
[40] Dirección de una página web almacenada en el navegador para agilizar su uso posterior.

defraudada. Por otro lado, de manera similar a los filtros de correo no deseado, los sitios fraudulentos pueden encontrarse alojados en los miembros de una red de bots, lo que hace muy complicada su erradicación.

A pesar de que muchas plataformas son inherentemente inseguras, muchos problemas podrían arreglarse con educación y concientización. La distribución de información referente a cómo mantener en secreto contraseñas, contraseñas de un solo uso y PINs, la importancia de mantener antivirus y sistemas operativos actualizados, etc., además de disminuir el riesgo de que los clientes realicen una acción que desemboque en una ataque, posibilita a las instituciones reducir la ventana en la que éstas deben asumir la responsabilidad en caso de un fraude.

### 2.2.2 Controles regulatorios

El uso de la tecnología no es suficiente en la administración del riesgo, porque sin la presencia de regulaciones y estándares inteligentes, hasta los mejores mecanismos pueden ser fácilmente evadidos.

La correcta selección de controles debe emanar de una óptima evaluación del riesgo y de las políticas que derivan de ella. Más aún, en varios casos se deben considerar igualmente las legislaciones locales e internacionales, que han ido creciendo y actualizándose a la par de la popularidad y proliferación de estos servicios electrónicos.

Entre los principales estándares y regulaciones que conciernen a la banca electrónica en Estados Unidos y en el ámbito internacional se encuentran los siguientes.

#### *2.2.2.1 Estándares*

- Autenticación en un entorno de banca electrónica. En el año 2001, el Consejo Federal de Evaluación de Instituciones Financieras formuló la guía para la autenticación en un entorno de banca electrónica. Esta guía, a pesar de que ha sido modificada a la par del avance en la tecnología, establece que los métodos de autenticación a utilizar en los diversos servicios bancarios ofrecidos deben ser congruentes con los riesgos asociados a dichos servicios, los cuales deben ser determinados a través de metodologías formales de análisis de riesgos.

- Estándar de seguridad de los datos de la Industria de Tarjetas de Pago. En el año 2004, con un acuerdo entre cinco de las principales instituciones financieras (Visa, Mastercard, American Express, Discover y el buró de crédito japonés), el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago fue fundado. Su estándar, que establece los niveles de seguridad mínimos que deben cumplirse en el almacenamiento, procesamiento y transmisión de datos por parte de los usuarios de tarjetas de crédito y débito, es resultado de la fusión de las políticas de seguridad pertenecientes a cada una de las instituciones fundadoras. En general, busca reducir el fraude en tarjetas de crédito debido a la exposición de información sensible.

- Principios de administración del riesgo para banca electrónica. El Comité de Supervisión Bancaria de Basilea, además de ser responsable de la emisión de los acuerdos internacionales referentes a leyes y regulaciones financieras (Basilea I, II y III), publicó en el año 2003 una guía cuya intención es promover la seguridad de

las actividades bancarias a través de medios electrónicos, así como expresar las expectativas regulatorias del propio comité [18].

La idea principal es procurar que las instituciones integren las actividades electrónicas dentro de sus marcos generales de administración del riesgo, adecuándolos a los nuevos canales de comunicación cuando sea necesario, en lugar de establecer criterios detallados, exclusivos y estrictos para los servicios adicionales. Con la finalidad de facilitar dicha integración, el comité propone los siguientes tres principios básicos:

- Supervisión por parte de la administración y junta de directores. Debido a que estas áreas son las encargadas de desarrollar estrategias de negocio, deben asegurarse de que las actividades electrónicas estén incorporadas a los objetivos estratégicos, que sus riesgos se encuentren identificados, que los procesos de mitigación y monitoreo asociados estén correctamente desarrollados y que evaluaciones constantes de los resultados en contraste con los planes previamente establecidos se lleven a cabo.

- Controles de seguridad. Las consideraciones técnicas emanadas de los procesos de seguridad desarrollados por la parte de negocio deben encontrarse implementadas a cabalidad, prestando especial atención a temas como autenticación, no repudio, integridad de datos y transacciones, segregación de funciones, administración de privilegios, pistas de auditoría y confidencialidad de información crítica.

- Administración del riesgo legal y de reputación. Las instituciones deben establecer las medidas adecuadas para cumplir con las responsabilidades que tienen con sus clientes, en referencia a la no divulgación de información, protección de datos personales y disponibilidad de los servicios, de manera independiente a las exigencias adicionales que se generen debido a leyes o regulaciones en cuya jurisdicción se encuentren operando.

#### *2.2.2.2 Regulaciones*

- Ley contra el fraude y abuso computacional. En sus orígenes, en el año 1984, tenía la intención de reducir la explotación de vulnerabilidades en sistemas y redes gubernamentales y de instituciones financieras, así como la persecución de delitos (acceso no autorizado, daño o amenaza de daño, robo y divulgación de información, fraude, espionaje) relacionados con tales sistemas.

- Ley de protección de las infraestructuras de información nacional. Formulada en 1996, establece la ilegalidad de los ataques de denegación de servicio y crea el Centro Nacional de Protección a la Infraestructura dentro de la Oficina Federal de Investigación (FBI, por sus siglas en inglés.)

- Ley sobre el uso de firmas electrónicas en el comercio global y nacional. Señala que a partir del año 2000, en que fue formulada, se autoriza el uso de la firma electrónica en documentos legales.

- Ley CAN-SPAM. Creada en el año 2003, provee el marco legal para interponer demandas contra distribuidores de correo electrónico no deseado, además de

que crea nuevas responsabilidades legales para atender situaciones en las que los perpetradores oculten su identidad y la fuente originadora de correo no deseado a los destinatarios, proveedores de servicios de internet o agencias de seguridad.

- U. S. Safe Web act. Expedida en el año 2006, concede a la Comisión Federal de Comercio de los Estados Unidos la habilidad de otorgar compensaciones monetarias a los consumidores en casos que involucren código malicioso, correo no deseado, fraude y engaño por internet. Adicionalmente, posibilita una mejor coordinación en investigaciones sobre estos temas con sus contrapartes extranjeras.

- Regla de banderas rojas para el robo de identidad. Fue creada por la Comisión Federal de Comercio de los Estados Unidos en el año 2008, aunque entró en vigor hasta el 2010. Establece que toda entidad que, directa o indirectamente, realice transacciones en las cuentas bancarias de un consumidor, debe desarrollar, implementar y administrar un programa de prevención de robo de identidad. Dicho programa debe definir las "banderas rojas" que afecten a la entidad, detectarlas en operación, prevenir y mitigar el robo de identidad una vez que las banderas han sido identificadas y actualizar el programa de manera constante.

Además de las regulaciones anteriores, algunas otras han sido propuestas y se encuentran en espera de ser aprobadas e implementadas:

- Ley de mejora a la ciberseguridad del 2010. Requiere al Instituto Nacional de Estándares y Tecnología y a la Fundación Nacional de Ciencia de los Estados Unidos el desarrollo de educación pública con miras en la concientización de los usuarios en temas de seguridad y estándares, además de iniciar programas de investigación y desarrollo de profesionales en ciberseguridad.

- Ley de seguridad de datos y notificación de brechas del 2010. Requiere a las organizaciones que almacenen información personal de individuales el adoptar las medidas apropiadas para la protección de tales datos y, además, requiere la notificación oportuna a las personas afectadas si se presenta un brecha de seguridad que comprometa su información.

Las leyes y estándares anteriores buscan establecer un marco regulatorio que sirva de guía de implementación y operación en la realización de transacciones electrónicas, así como de respaldo legal para la persecución y sanción de los nuevos delitos que el uso de la tecnología ha generado, ayudando a las instituciones en su búsqueda para alcanzar los niveles de seguridad más óptimos en el ofrecimiento de sus servicios.

En el caso mexicano, las leyes en la materia no se encuentran en un punto tan avanzado como las de nuestros vecinos del norte y, más aún, las asociaciones preocupadas por las temáticas de seguridad son extremadamente pocas y no cuentan con estándares publicados. A pesar de lo anterior, existen igualmente legislaciones que proveen un marco jurídico para las operaciones en medios electrónicos.

La ley de instituciones de crédito, en sus artículos 52 y 100 establece la posibilidad de que las instituciones bancarias ofrezcan sus servicios a través de medios electrónicos, siempre y cuando señalen de modo contractual la manera en que operarán y los riesgos inherentes a la utilización de dichos servicios, las formas de identificar al usuario, así como los derechos y obligaciones de las partes involucradas. Asimismo, decreta que los medios de identificación utilizados tendrán los mismos efectos que una firma autógrafa.

Adicionalmente, permite que las instituciones almacenen la información referente a todas las transacciones electrónicas, en los medios que la Comisión Nacional Bancaria y de Valores (CNBV) autorice, como documentos probatorios en juicio.

De manera similar, el código de comercio en su título segundo establece igualmente reglas a través de las cuales las transacciones en medios electrónicos deben llevarse a cabo, además de señalar que los registros generados por estas transacciones pueden utilizarse como prueba en alguna disputa.

Las legislaciones anteriores, siendo obra de congresos de diversos períodos, mencionan de manera muy general las disposiciones a atender en la banca electrónica, haciendo referencia en varias ocasiones a la autoridad de la CNBV, que al ser un organismo especializado, es la encargada de profundizar en la problemática y establecer con todo detalle los mecanismos necesarios para llevar a cabo este tipo de transacciones de forma segura a través del capítulo diez de su Circular Única de Bancos.

Dentro de las disposiciones más importantes en esta regulación, adicionales a lo señalado en la ley de instituciones de crédito y el código de comercio, se encuentran las siguientes:

- Para iniciar una sesión de banca en línea se deben solicitar y validar un identificador de usuario (de al menos 6 caracteres para banca electrónica y el número de teléfono para banca móvil) y un factor de autenticación de categoría 2 ó 4.

- Las instituciones deben proveer lo necesario para impedir que la información de identificación y autenticación puede ser leída en la pantalla de los dispositivos de acceso, de lo contrario, todo riesgo y costo derivado de operaciones no reconocidas será asumido por las propias instituciones.

- Deberán implementarse cuatro posibles factores de autenticación que se utilizarán de manera individual o en conjunto, dependiendo del medio y la transacción a realizar.

    - Categoría 1. Información obtenida mediante la aplicación de cuestionarios verbales a los usuarios (Para banca a través de línea telefónica únicamente.)

    - Categoría 2. Información que sólo el usuario sabe e ingresa a través de su dispositivo de acceso (contraseñas y NIP.)

    - Categoría 3. Información contenida o generada por medios o dispositivos electrónicos, proporcionados por las instituciones a sus usuarios (generadores de contraseñas dinámicas y de un solo uso.)

    - Categoría 4. Información derivada de las propias características físicas de los usuarios.

- Las instituciones deben establecer mecanismos para que sus usuarios de banca por internet puedan autenticar a las propias instituciones.

- Las instituciones deben solicitar un segundo factor de autenticación de categoría 3 ó 4, diferente de los utilizados para acceder a los servicios de banca por internet, para confirmar y autorizar transacciones solicitadas por el usuario. Una excepción a lo anterior son los micro pagos a través de dispositivos móviles o terminal de

punto de venta, en cuyo caso las instituciones asumen los riesgos y los costos de operaciones no reconocidas.

- Las instituciones deben proveer lo necesario para que, una vez autenticado un usuario, la sesión no pueda ser utilizada por un tercero. Adicionalmente, debe dar por terminada la sesión de manera automática cuando se presente un periodo de inactividad establecido para cada servicio y debe bloquear todos los factores de autenticación cuando el número de intentos de acceso erróneos sea igual a cinco consecutivos o cuando el servicio haya dejado de utilizarse por un largo período.

- Las instituciones tienen prohibido solicitar los datos de autenticación de sus usuarios, así como contar con mecanismos que les permita recuperarlos de algún modo.

- Cuando las instituciones pongan al alcance de los usuarios equipos electrónicos o de telecomunicaciones para la realización de banca electrónica, debe adoptar medidas para impedir la instalación de cualquier dispositivo o programa que interfiera con el manejo de la información de los usuarios.

- Las instituciones deben implementar mecanismos de seguridad en la transmisión, almacenamiento y procesamiento de la información, utilizando medios de comunicación cifrada, cifrado de factores de autenticación y haciéndose responsables de la distribución de llaves cuando éstas sean necesarias.

- Las instituciones deben contar con estrictos controles de acceso a las bases de datos y archivos correspondientes a las operaciones efectuados en medios electrónicos.

- Las instituciones deben mantener mecanismos de monitoreo para identificar y prevenir eventos que se aparten de los parámetros del uso habitual de los usuarios. Además, toda incidencia, falla o vulnerabilidad detectada debe mantenerse en bitácoras y bases de datos por un período de al menos cinco años.

- Las instituciones deben realizar revisiones de seguridad para verificar la suficiencia de los controles aplicados a su infraestructura de banca electrónica al menos una vez al año, o cuando se realicen cambios significativos en los sistemas que proveen los servicios bancarios.

- Las instituciones deben procurar la operación continua de la infraestructura y contar con procedimientos de respuesta a incidentes de seguridad, así como dar pronta solución para restaurar los servicios si éstos han sido deshabilitados.

No es casualidad que las regulaciones anteriores cubran de manera general las vulnerabilidades y controles mencionados a lo largo del capítulo. Cada una de ellas emana de un análisis del riesgo no sólo a nivel de operaciones, sino que en algunos casos (como las legislaciones estadounidenses), elevan la problemática a niveles de seguridad nacional y, como toda metodología de análisis de este tipo, se encuentran en constante revisión y actualización.

# 3. Análisis de riesgos

Toda actividad realizada en cualquier ámbito tiene asociados riesgos[41] de diversos tipos, de manera inherente. Con la finalidad de evitar las consecuencias que la materialización de dichos riesgos implicaría, es del profundo interés de cualquier organización el reducirlos hasta un nivel considerado como aceptable.

Pero, ¿Cómo identificar las características débiles y las consecuencias indeseables en un sistema[42]?, ¿Cómo reducirlas y cómo determinar los niveles de riesgo óptimos?

## 3.1 Evolución

Antes de la década de los 40, la aproximación utilizada para esta problemática se limitaba a atender únicamente las amenazas más evidentes durante las fases de diseño de los sistemas y corregir problemas conforme se fueran presentando en el uso normal de los mismos o en la fase de pruebas, es decir, una suerte de "prueba y error". Sin embargo, al comenzar a proliferar proyectos con una criticidad muy alta (en los campos aeroespacial, militar y nuclear, por nombrar algunos) pronto fue evidente que esta aproximación no era adecuada, debido a que las consecuencias de una falla serían catastróficas.

Los esfuerzos para establecer una manera formal para alcanzar la seguridad en sistemas comenzaron en la década de los años 60 en instituciones como el Departamento de Defensa y la Administración Nacional de Aeronáutica y del Espacio (NASA, por sus siglas en inglés) en los Estados Unidos, a través del desarrollo de programas y documentos en los que se detallaban los requerimientos de seguridad que estas agencias federales establecían para sus sistemas, subsistemas y equipamiento, creando así las primeras metodologías de análisis de riesgos. Otras instituciones, como el Departamento de Energía, fueron incorporándose a esta iniciativa a lo largo de la siguiente década, conjuntando las mejores características de los programas ya existentes, tanto para su uso interno como para establecer un estándar entre sus contratistas.

Para el inicio de la década de los 80, estas metodologías llamaron la atención de otro tipo de instituciones, como la industria petrolera, debido a que la mejora en los diseños y, por tanto, de la seguridad en los sistemas de las agencias federales comenzó a ser evidente. Si bien sus proyectos no alcanzaban el mismo nivel de criticidad, el alto costo que representaban justificaba la inversión a mediano plazo en el desarrollo de un análisis propio de este tipo.

La evolución de los programas al final del siglo pasado incluyó los procesos y hasta el aseguramiento de la calidad en industrias como la química, donde malas prácticas o impurezas en cualquier fase, podían producir una reacción no deseada, en perjuicio directo a trabajadores, clientes e institución. En los últimos años, las metodologías de análisis de riesgos han volcado sus esfuerzos en alcanzar una seguridad construida en un y para un sistema desde las fases de diseño del mismo y, conforme la noción de activo[43] para las instituciones se modifica y amplía, son aplicadas en actividades con objetivos y características muy específicas, como la seguridad de la información [19, pp. 3-7].

[41] Posibilidad de ocurrencia de un daño o pérdida.
[42] Conjunto de personas, procesos, hardware, software, etc. dentro de un entorno, con una tarea específica en común.
[43] Todo aquello con valor para una organización.

## 3.2 Definiciones

Un factor en común durante la evolución de las metodologías de análisis de riesgos es que cada entidad desarrolló su propio programa de manera independiente, de acuerdo a sus necesidades. Si bien esta práctica es común aún en nuestros días, en la mayoría de las ocasiones provoca una falta de estandarización en conceptos y prácticas, por lo que es complicado proporcionar definiciones consensuadas. El ámbito de la seguridad informática no es la excepción y varias de las instituciones más reconocidas en el área ofrecen sus respectivas propuestas, como las que a continuación se enuncian.

De acuerdo al ISO[44] 27001-2005, un análisis de riesgos es *el uso sistemático de información disponible como base para la evaluación, el tratamiento y la aceptación del riesgo, identificando orígenes y estimando la frecuencia y magnitud de sus consecuencias* [20, p. 11].

Por otro lado, para el Instituto de Ingeniería de Software de la Universidad Carnegie Mellon, a través de su metodología OCTAVE[45], es *el proceso continuo de identificar riesgos e implementar planes para atenderlos* [21, p. 124].

Finalmente, el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) de los Estados Unidos, a través de su publicación especial 800-39, considera que es *el programa y procesos de apoyo para administrar el riesgo de la seguridad de la información en las operaciones organizacionales (incluyendo misión, funciones, imagen, reputación), activos, individuos, otras organizaciones y la Nación misma. Incluye el establecimiento del contexto de las actividades riesgosas, la evaluación, respuesta y monitoreo continuo del riesgo* [22, pp. B-8].

¿Qué ideas tienen en común las definiciones anteriores?

- No se mencionan acciones únicas, sino se habla de procesos sistemáticos y continuos.
- Se parte de la identificación de los riesgos y de su contexto.
- Se evalúan los riesgos identificados, considerando probabilidades e impacto.
- Se desarrollan planes para atender los riesgos más significativos.

Considerando lo anterior, una metodología de análisis de riesgos podría definirse como un proceso continuo que tiene como finalidad la identificación de vulnerabilidades[46] en un sistema, el cálculo del impacto que significaría la manifestación de alguna de las amenazas[47] a la que éste se encuentra expuesto y determinar apropiadamente si existe la necesidad de adoptar medidas preventivas para reducir los riesgos de alguna actividad a un nivel aceptable.

[44] Organización Internacional para la Estandarización (International Organization for Standardization.)
[45] Evaluación de Amenazas Operacionalmente Críticas, Activos y Vulnerabilidades (Operationally Critical Threat, Asset, and Vulnerability Evaluation.)
[46] Debilidad, defecto o falla.
[47] Evento con el potencial de causar algún daño.

## 3.3 Tipos de análisis de riesgos

Existen esencialmente dos aproximaciones para realizar un análisis de riesgos, cada una con diferentes ventajas y desventajas, de acuerdo al contexto en el que sean utilizadas.

Un análisis cuantitativo emplea métricas numéricas, generalmente expresadas en términos monetarios o probabilísticos. Se trata de un análisis crítico y objetivo que se basa en una gran cantidad de información y técnicas matemáticas para establecer la posibilidad e impacto de sucesos negativos. A través de este tipo de análisis puede demostrarse con facilidad el costo-beneficio de las acciones preventivas de una organización, sin embargo, el tiempo y esfuerzo que se debe dedicar es considerable, debido principalmente a que los cálculos y análisis necesarios son usualmente complejos.

En contraste, un análisis cualitativo emplea únicamente métricas descriptivas, como "alto", "medio" o "bajo", para caracterizar la magnitud de consecuencias y la posibilidad de que se concreten. Debido a su carácter subjetivo, no es muy útil para demostrar costo-beneficio, pero puede ser utilizado para identificar previamente riesgos que necesitan un análisis más detallado, cuando no se cuente con la información suficiente para realizar un análisis cuantitativo o cuando el nivel del riesgo no justifica los esfuerzos requeridos en un análisis a profundidad. La calidad de este tipo de análisis depende en gran parte de la habilidad de aquellos que lo realizan y del consenso previo para definir el valor adecuado de las métricas [23].

## 3.4 Fases de los análisis de riesgos

Como se mencionó anteriormente, en la actualidad existen varias propuestas de metodología de análisis de riesgos provenientes de diferentes instituciones. Sin embargo, a pesar de que todas ellas difieren en cuestiones como cantidad de fases o prácticas, se apegan a los puntos genéricos siguientes:

1. Establecimiento del contexto. Es importante especificar claramente el alcance del análisis, así como definir previamente la terminología que se utilizará a lo largo del mismo, para evitar complicaciones derivadas de la falta de estandarización presente en estas metodologías.

2. Identificación.

    a) De activos. El primer paso es la creación de un listado de los activos (hardware, software, datos, documentación, servicios, entre otros) que se desean proteger, las relaciones que hay entre ellos y su valor, que puede ser asignado en base a varios criterios.

    En el caso de los activos tangibles, la manera más directa de asignarles valor es a través del costo de adquisición y manutención, aunque en la mayoría de las ocasiones se toman en consideración variables como las ganancias que el bien produce, las pérdidas si no se encuentra disponible, el costo de reemplazarlo si sufre algún daño y hasta los costos y pérdidas potenciales que una demanda derivada del compromiso de éste suscitaría [24].

    Por otro lado, la valuación de un activo intangible es un tanto más complicada. Un método consiste en la comparación del bien (por ejemplo, una marca) con otros de características similares en el mercado para

establecer un valor aproximado en base a sus transacciones económicas. Otra aproximación se basa en la cotización en bolsa de valores del intangible, en caso de que sea aplicable. Una consideración más, que es muy utilizada, establece el valor del activo a través de las ganancias que éste genera para el negocio [25].

En la práctica, tanto para activos tangibles como intangibles, se utiliza una combinación de varios de los criterios mencionados para llegar a una métrica lo más realista posible.

El listado obtenido tras concluir esta fase debe ser actualizado de manera regular con llegada de nuevo equipo, modificación de infraestructura, etc.

b) De amenazas. Una vez definidos los activos de interés para el análisis, se determinan las amenazas a los que éstos se encuentran expuestos y el impacto que la culminación de alguna de ellas representaría, sin dejar de considerar tanto riesgos propios de los sistemas como factores humanos.

Para concretar las actividades anteriores se requiere un profundo conocimiento del sistema en estudio, que puede ser adquirido mediante la exposición a todos los procesos del mismo (lo cual requiere una cantidad de tiempo significativa y abre la posibilidad a la omisión de detalles importantes) o con el apoyo de los responsables de cada una de las áreas o expertos en la temática.

Las consultas con terceros pueden realizarse a través del fomento de una lluvia de ideas, referente a cuáles son los activos relevantes en una organización, qué se hace para protegerlos y qué prácticas inadecuadas persisten. La información recopilada es consolidada posteriormente, obteniendo así perfiles de activos críticos, sus vulnerabilidades, amenazas y requerimientos de seguridad [21, p. 36].

El contar con reportes de accidentes previos o de riesgos característicos de cada sector es un recurso muy útil en el desarrollo de esta fase, debido a que la información que contienen se basa en hechos reales y establece precedentes para atender efectos parecidos posteriores.

3. Evaluación.

a) Priorización de amenazas. La criticidad de una amenaza se establece en función de su probabilidad de ocurrencia y de la importancia del activo en el que pueden consolidarse. La clasificación de amenazas permite definir qué riesgos merecen ser atendidos y la prioridad que debe asignarse a cada uno de ellos.

Una manera de lograr lo anterior es a través de tablas que relacionen los dos factores antes mencionados (Tabla 1) con métricas cuantitativas o cualitativas acordadas previamente (Tabla 2.)

| | Probabilidad de consolidación de amenaza | | |
|---|---|---|---|
| Importancia del activo | Baja | Media | Alta |
| Baja | No crítica | No crítica | Poco crítica |
| Media | No crítica | Poco crítica | Crítica |
| Alta | Poco crítica | Crítica | Muy crítica |

Tabla 1. Ejemplo de tabla cualitativa para asignar prioridades a amenazas.

| Prioridad de amenaza | No crítica | Poco crítica | Crítica | Muy crítica |
|---|---|---|---|---|
| Valoración | 1 | 2 | 3 | 4 |

Tabla 2. Ejemplo de tabla cualitativa para asignar una métrica a la prioridad de las amenazas.

b) Estimación del impacto total. No basta con identificar la criticidad de las amenazas, sino que es necesario calcular igualmente el efecto (monetario o en reputación) que la consolidación de alguna tendría en la organización. Es necesario emplear las mismas métricas utilizadas al priorizar para mantener la consistencia del análisis.

   Para este fin, las llamadas "hojas de factor de riesgo" (Tabla 3) son muy utilizadas, de manera tanto cualitativa como cuantitativa [26, p. 26].

| Amenaza | Prioridad de amenaza | Impacto a la organización | Factor de riesgo estimado |
|---|---|---|---|
| Amenaza 1 | 2 | 2 | 4 |
| Amenaza 2 | 4 | 4 | 8 |

Tabla 3. Ejemplo de hoja de factor de riesgo con métricas cualitativas.

   En el ejemplo anterior, el impacto a la organización fue establecido utilizando el criterio de la priorización de amenazas, mientras que el factor de riesgo es resultado de la suma de ambos valores. Cuando éste es mayor a un límite previamente establecido, la amenaza a la que está asociada será considerada dentro del grupo con prioridad de atención en la selección de medidas de protección.

4. Selección de medidas de protección. Una vez plenamente identificadas vulnerabilidades y amenazas, es necesaria la selección de controles[48] que las mitiguen. La necesidad de controles no sólo emana del análisis de riesgos, sino también deben considerarse requerimientos legales, regulatorios o contractuales y los principios y objetivos de la organización. Éstos pueden ser de carácter técnico, administrativo, legal o físico, pero todos tienen la consigna de proteger activos a un costo razonable y conforme a las amenazas identificadas como de mayor riesgo.

   Para determinar qué controles proveen el máximo nivel de protección al menor costo, se puede utilizar igualmente una tabla que relacione el impacto a la organización de cada amenaza con el costo de implantación de un determinado control, el cual debe ser menor al valor de las posibles pérdidas (Tabla 4.) Adicionalmente, es importante considerar las consecuencias de seleccionar una medida de protección específica, como su administración, la capacitación requerida, su efecto en la productividad de las operaciones, etc. [26, p. 32].

[48] Medida de protección, técnica o normativa, de los activos informáticos.

El resultado de la aplicación de controles no es la obtención de una seguridad completa de los activos más importantes, sino la reducción de sus riesgos a niveles aceptables. Estos riesgos residuales[49], además de ser asumidos, pueden ser transferidos a un tercero a través de alguna relación contractual para tal fin.

| Amenaza | Factor de riesgo estimado | Posible solución | Costo |
|---|---|---|---|
| | | | |
| | | | |

Tabla 4. Ejemplo de tabla para priorizar controles.

5. Monitoreo. Como se mencionó en las definiciones iniciales, un análisis de riesgos es un proceso continuo, por tanto, no basta con la identificación de activos, vulnerabilidades y amenazas o con la implementación de controles, sino que debe establecerse una estrategia de monitoreo continuo para verificar el cumplimiento, la efectividad o la necesidad de modificación de las soluciones implementadas. Este monitoreo puede ser manual o automático, con la frecuencia que la organización requiera de acuerdo a su necesidad de retroalimentación.

6. Reporte de resultados. El último paso consiste en poner por escrito los resultados del análisis realizado, incluyendo en éstos los niveles de vulnerabilidad identificados, amenazas, su frecuencia e impacto, controles y sus costos, así como los riesgos residuales al final de la metodología. Este tipo de documentos es de gran utilidad, ya que permite la creación de un archivo histórico que apoye las decisiones de análisis futuros.

Como puede observarse, un análisis de riesgos es un ciclo constante de planeación, acción, verificación y modificación. No es un fin en sí mismo, sino que es el punto de partida de la acción preventiva de una organización para actuar antes de que efectos negativos se presenten, evitando costos sociales y económicos.

## 3.5 Dificultades y futuro

A pesar de que la utilización y aceptación de las metodologías de análisis de riesgos en un gran número de áreas y actividades es cada día mayor, aún existen factores que impiden su desarrollo total.

La estandarización es casi nula o se da únicamente en grupos de instituciones afines que realizan acuerdos para alcanzar cierto nivel de interoperabilidad. En muchas ocasiones cada agencia, contratista, analista, etc. tiene su propio conjunto de definiciones, técnicas, métricas, escalas o nomenclaturas. Si bien la práctica de desarrollar metodologías hechas a la medida es muy común, sería de gran utilidad el poder seleccionar de entre un conjunto común de recursos (definiciones, técnicas, formatos, hojas de trabajo, etc.) aquellos que se adecúen mejor a cada necesidad.

Otro de los problemas radica en la falta de educación y entrenamiento. Existen pocos ingenieros calificados debido a que un número muy reducido de escuelas ofrecen cursos de análisis de riesgos, lo que reduce la oferta educativa a programas "de la casa" a través de organizaciones privadas, que aún así se enfrentan a la ausencia de un conjunto

[49] Aquel riesgo que permanece aún al finalizar un proceso de análisis de riesgos.

de conocimientos en común para impartir, debido nuevamente a la falta de estandarización [19, pp. 43-55].

La resolución de este tipo de problemas a mediano plazo ayudará a que estas metodologías dejen de ser consideradas un arte, se acerquen a la clasificación de ciencia y que la calidad de los productos de los análisis dependan más del apego a procedimientos estandarizados que a las habilidades de un analista.

## 3.6 Técnicas de análisis: Árboles analíticos

Dentro del gran número de técnicas existentes para implementar las fases de un análisis de riesgos, los llamados "árboles analíticos" son una de las más utilizadas debido a la claridad con que pueden expresarse los componentes, relaciones, requerimientos y alternativas en un sistema, así como la información resultante del análisis, que es de gran valor para la toma racional de decisiones en varias etapas de diversos proyectos y como registros reusables a futuro. [19, pp. 105-107].

Son una manera de representar sistemas gráficamente y propician el uso del razonamiento deductivo para identificar las rutas críticas que pueden existir desde un evento general hasta los eventos específicos que lo producen. Son llamados "árboles" porque su estructura asemeja esta forma: una raíz representando el evento de análisis y su desarrollo a través de diversas ramas que desembocan en hojas que simbolizan incidencias concretas que llevan a él.

Existen dos tipos de árboles analíticos:

- Árboles positivos. Son desarrollados para verificar que un sistema funciona adecuadamente.

- Árboles negativos. También llamados árboles de fallas, son desarrollados para investigar y solucionar fallas en los sistemas.

Como se mencionó anteriormente, uno de los principales intereses de un análisis de riesgos es la identificación de amenazas y vulnerabilidades en un sistema, por lo que el uso de un árbol analítico negativo es de mayor pertinencia en este contexto.

### 3.6.1 Árboles de fallas

Un árbol de fallas es un marco lógico para expresar combinaciones de incidentes negativos en los componentes de un sistema que pueden derivar en estados no deseados, eventos no intencionados o en el fallo total de éste [27, p. 3].

Su estructura de árbol está constituida por un accidente o falla principal en el nodo raíz, estados de falla o accidentes menores en los nodos internos y eventos básicos o fallas de componentes específicos en las hojas.

Todos los diferentes tipos de eventos (fallas concretas, eventos normales inherentes a los sistemas, efectos del ambiente, componentes de hardware, software, humanos y procesos) están ligados a través de bloques constructores que buscan identificar las relaciones causa-efecto entre ellos (Figura 4):

- Rectángulo. Representa el evento principal o cualquiera de los eventos secundarios que pueden derivar en él. Este tipo de bloque debe tener puertas lógicas y eventos de entrada asociados.

- Círculo. Representa una falla básica de algún componente de un sistema. No requiere ningún desarrollo, por lo que no tiene ni puertas lógicas ni eventos de entrada asociados.

- Rombo. Representa una falla básica que, por falta de información, información incompleta o poca relevancia, no se encuentra desarrollada.

- Puerta AND. Representa una puerta lógica en la que el evento de salida ocurre únicamente si todos los eventos de entrada ocurren simultáneamente.

- Puerta OR. Representa una puerta lógica en la que el evento de salida ocurre si uno o más de los eventos de entrada ocurren.

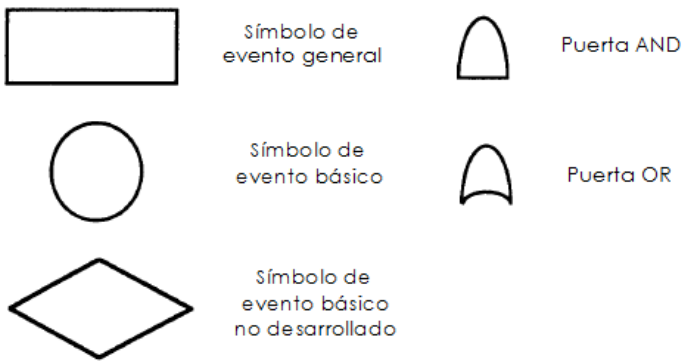


Figura 4. Bloques constructores de un árbol de fallas.

La creación de un árbol de fallas comienza con una definición muy específica del evento no deseado a analizar y de los componentes e incidencias críticas que contribuyen en mayor medida a que se suscite. Posteriormente se identifican todas las posibles causas del evento, así como las relaciones entre ellas y los componentes críticos antes establecidos.

La evaluación matemática de un árbol creado varía de acuerdo al tipo de análisis que se realice. Una aproximación cualitativa se limita a la identificación de componentes críticos y a su expresión en base al álgebra booleana, mientras que la aproximación cuantitativa incluye además el cálculo de probabilidades de ocurrencia de cada evento (Figura 5.)

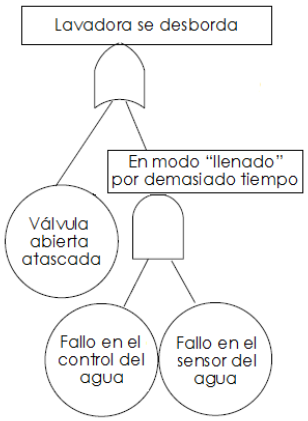


Figura 5. Ejemplo de un árbol de fallas básico.

El ejemplo anterior presenta el desbordamiento del agua en una lavadora convencional como el evento a analizar.

Dos posibles razones para que el hecho se suscite son que la válvula que provee el agua se atasque mientras se encuentra abierta o que el sistema entre en "modo llenado" por demasiado tiempo. Tanto la falla del componente básico como el evento secundario están ligados al evento raíz a través de una puerta OR, lo que implica que sólo es necesario uno de los eventos de entrada para lograr el evento de salida. Por otro lado, para que el modo "llenado" se suscite el tiempo suficiente para desbordar la lavadora, es necesario que tanto el sensor de medición del agua como el sistema de control de la misma fallen, por tanto están ligados al evento secundario por una puerta AND.

Su evaluación cualitativa constaría de la relación lógica entre los eventos básicos y el evento raíz:

Falla general (F) = Falla de válvula (A) OR [Falla de control (B) AND Falla de sensor (C)],

que se puede parametrizar como:

$F = A + BC$

Al agregar cálculos probabilísticos sobre la función booleana se cubre la perspectiva cuantitativa, de la siguiente manera:

$Pr[F] = Pr[A + BC]$
$Pr[F] = Pr[A] + Pr[BC] – Pr[ABC]$

Si, por ejemplo, $Pr[A] = 0.01$, $Pr[B] = 0.05$ y $Pr[C] = 0.075$, entonces:

$Pr[F] = 0.01 + (0.05 * 0.075) – (0.01 * 0.05 * 0.075) = 0.0137125$

Siendo así, existe aproximadamente un 1.37% de probabilidad de que el nivel del agua se desborde, considerando los factores de riesgos establecidos [27, pp. 7, 8].

Para que la información que provee un árbol de fallas sea válida y útil, éste debe ser constantemente revisado durante su creación, evaluación y actualización por aquellos

que conocen a la perfección el sistema que se analiza, quienes a su vez deben ser capaces de interpretar correctamente los resultados obtenidos.

Si bien este tipo de análisis es una excelente herramienta para evaluar un sistema, tiene la desventaja de que tanto los eventos a analizar como los factores que los provocan deben ser previstos, por tanto, como todo análisis de riesgos en la actualidad, su éxito depende en gran medida del analista que construye, evalúa e interpreta el árbol.

Finalmente, es importante hacer notar que éste no es un análisis de amenazas y no modela ataques[50], sino que recrea un estimado de la realidad de un sistema y sus fallas, limitándose además a las relacionadas con el evento raíz establecido únicamente [28, pp. 5-15]. Sin embargo, es el punto de partida para análisis que sí atienden estas necesidades, como los llamados "árboles de ataque".

### 3.6.2 Árboles de ataque

Un árbol de ataque es una manera formal y metódica para describir la seguridad de los sistemas modelando las amenazas a las que se encuentran expuestos, calculando su probabilidad de ocurrencia y diseñando las contramedidas adecuadas [29].

Comparte la estructura propia de los árboles de fallas, difiriendo de ellos en que en la raíz no se establecen eventos de falla, sino las metas de un atacante y en que las hojas no simbolizan eventos básicos o fallas de componentes, sino ataques concretos que pueden derivar en la consecución de metas secundarias en los nodos internos y, en última instancia, de la meta principal.

Aunque no cuentan con la misma cantidad de bloques constructores, un árbol de ataque igualmente identifica las relaciones causa-efecto entre ataques y metas, a través de dos tipos de conexiones lógicas:

- Conexión AND. Representan los pasos requeridos para alcanzar la meta superior. Es necesario que todos los ataques o eventos inferiores ocurran simultáneamente.

- Conexión OR. Representan alternativas para alcanzar la meta superior. Es necesario que uno o más de los ataques o eventos inferiores ocurran.

Para crear un árbol de ataque se parte de la identificación de una meta principal a alcanzar dentro del sistema en estudio y de todos los posibles ataques que contribuyan a lograr tal objetivo u objetivos secundarios que en última instancia deriven en él.

A diferencia de los árboles de fallas, en los que se analiza únicamente la probabilidad de éxito o fracaso en la respuesta de un sistema ante una eventualidad [30, p. 3], en los árboles de ataque pueden realizarse varios tipos de análisis a través de otras tantas métricas.

Una evaluación cualitativa se basa en métricas booleanas, como "posible", "imposible", "fácil", "difícil", "barato", "costoso", entre otras. Por el contrario, una evaluación cuantitativa considera métricas continuas que no se limitan a cálculos probabilísticos, como el costo de realización de un ataque o el tiempo que el mismo requiere. En ambos

[50] Intento de destruir, exponer, alterar, deshabilitar, robar, o ganar acceso no autorizado a un activo.

casos es necesaria la propagación "hacia arriba" de las métricas definidas, es decir, desde las hojas y hacia la raíz (Figura 6.)

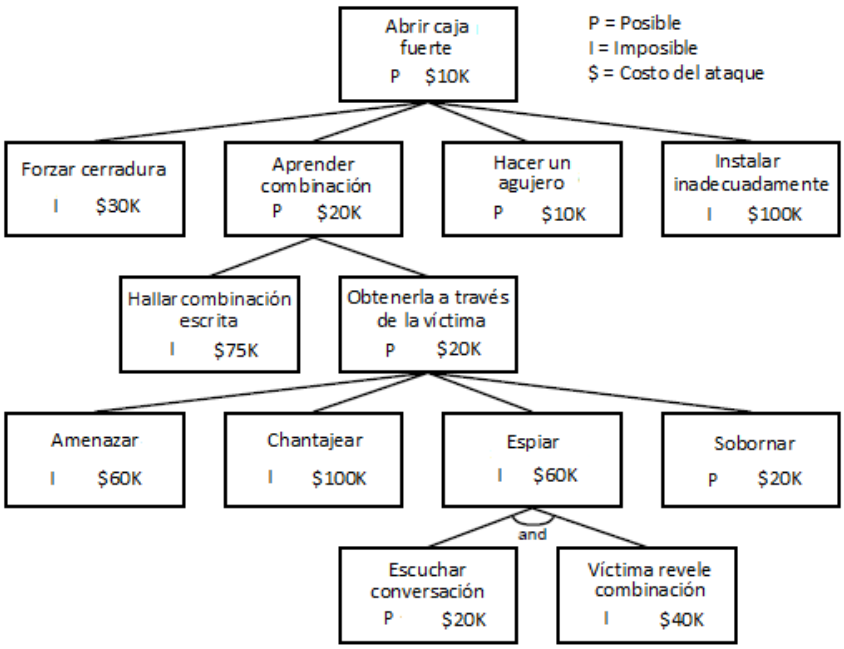


Figura 6. Ejemplo de un árbol de ataque básico.

El ejemplo anterior presenta el abrir una caja fuerte sin autorización como la meta a analizar.

Existen cuatro posibles alternativas para lograr la meta principal: forzar la cerradura, hacer un agujero en la caja, lograr que de alguna manera una instalación incorrecta la haga vulnerable o aprender la combinación de algún modo. Esta última opción, a su vez, puede ser conseguida si se encuentra la combinación escrita en algún lugar o a través de la amenaza, el chantaje, el soborno o el espionaje a la víctima. Dado que los eventos mencionados son diferentes alternativas para llegar a su nodo superior, se encuentran ligados a él a través de conexiones OR. Por otro lado, para obtener la combinación exitosamente a través del espionaje no sólo es necesario escuchar una conversación de la víctima, sino que dentro de ella se mencione la información que al atacante le interesa, por tanto, ambos eventos están ligados a su nodo superior con una conexión AND.

Pueden observarse también métricas tanto cualitativas ("posible" e "imposible") como cuantitativas (costo de realización del ataque). Cada una de ellas se propaga de manera diferente: como ya se mencionó, basta con que una de las alternativas con conexión OR sea posible para que el evento superior lo sea también y, en lo referente a costo, un atacante siempre buscará obtener el mayor beneficio con la menor inversión, por lo que es la alternativa más barata la que se propaga hacia arriba. Por el contrario, todos los eventos con conexión AND deben ser posibles para que el superior lo sea también y, por tanto, el costo se propaga hacia arriba como la suma de los costos inferiores.

La combinación de las métricas adecuadas puede proveer de una gran cantidad de información que facilita la toma de decisiones de seguridad. En el ejemplo, la métrica booleana indica que sólo dos ataques son posibles, sin embargo, "hacer un agujero" es el

que representa un menor costo de realización y al que se debe asignar mayor prioridad al implementar mecanismos de protección [31, pp. 9-22].

La caracterización de los posibles atacantes es también de gran ayuda para la toma de decisiones. Las diferencias en motivación, habilidad, financiamiento o nivel de riesgo a tolerar también permiten definir la criticidad de las ramas de un árbol [31, pp. 4-6]. Por ejemplo, un estudiante que prueba herramientas de ataque en su red escolar no tiene la misma motivación ni el financiamiento que un miembro del crimen organizado, por lo que el encargado de la seguridad de un campus no debe dedicar demasiada atención a ataques que sean muy caros de realizar o ilegales, dado que el alumno probablemente no desea ir a prisión.

Esta técnica, al ser un análisis de amenazas, cubre las carencias que los árboles de fallas presentan. Su generalidad y fundamento posibilita su aplicación en una gran cantidad de sistemas, aplicaciones y procesos, además de que la dota de una gran reusabilidad. Toda meta a analizar implica la construcción de un árbol diferente, cada uno de los cuales puede ser considerado como un módulo que puede formar parte de un árbol de ataque más complejo y más elaborado.

Como todo árbol analítico, cuenta con la desventaja de que sólo puede incluir eventos previstos y conocidos por aquel que realiza el análisis, por lo que una investigación previa extensa es requerida. En algunas ocasiones se utilizan repositorios[51] de ataques para disminuir la posibilidad de olvidar alguno.

Es requerida de igual manera una actualización constante de todos los elementos del árbol. El constante avance en la tecnología puede provocar que un ataque antes considerado como imposible o excesivamente costoso sea viable a corto plazo, por lo que verificar las métricas y sus cálculos, las conexiones lógicas, así como los impactos en las metas de los atacantes es necesario.

La seguridad no es un producto, es un proceso. Esta técnica, los árboles de ataque, contribuyen a un amplio entendimiento de tales procesos [29].

[51] Sitio centralizado donde se almacena y mantiene información digital.

# 4. Análisis del riesgo en el uso de la banca electrónica mediante árboles de ataque

En capítulos anteriores se ha hecho notar que, si bien la oferta de servicios bancarios a través de medios electrónicos es de gran importancia para las instituciones en la actualidad y por tanto la protección de los mismos es indispensable, en muchas ocasiones se prioriza funcionalidad sobre seguridad, facilitando el uso de los sistemas para los cuentahabientes y procurando protegerlos de las amenazas más críticas.

Pero, ¿Tales amenazas están realmente cubiertas?, ¿Los análisis costo – beneficio en la implementación de controles están correctamente realizados?, ¿Las regulaciones son suficientes o exceden la dimensión de la problemática?

El presente capítulo busca realizar un estudio de estas interrogantes a través de las metodologías de análisis de riesgo aplicadas al uso de la banca electrónica, utilizando principalmente la herramienta de árboles de ataque.

## 4.1 Justificación

Anteriormente se han presentado las características de los árboles analíticos y de ataque, sin embargo, es adecuado hacer énfasis en los beneficios de su contextualización en la banca electrónica móvil.

La iniciativa de utilizar esta herramienta en los análisis de riesgos presentes en este trabajo, se basa en la gran cantidad de información que éstos pueden proveer cuando se construyen adecuadamente, así como en su gran versatilidad y reusabilidad.

Lo anterior es muy conveniente tomando en cuenta los diferentes fraudes a la banca electrónica que se han presentado en los últimos años, lo cual demuestra que los vectores de ataque a los que se encuentra expuesta no se mantienen estáticos, sino que se adaptan a los avances en las medidas de protección.

De manera similar, un árbol de ataque es un documento vivo en constante actualización, por lo que aún cuando surjan nuevas amenazas o las ya existentes se tornen más fáciles de realizar, siempre se mantiene una adecuada visibilidad que permite la correcta toma de decisiones de seguridad por parte de aquellos encargados de administrarla.

## 4.2 Establecimiento del contexto

El objetivo principal de este trabajo es el estudio de los riesgos en el uso de la banca móvil, que forma parte de la banca electrónica. Sin embargo, una primera aproximación a la problemática se realizará a través del análisis del riesgo en los servicios bancarios por medios electrónicos utilizando computadoras personales, con la finalidad de apreciar con claridad los antecedentes, tanto positivos como negativos, presentes en esta modalidad de banca, así como verificar si éstos se mantienen o modifican al utilizar dispositivos móviles.

Adicionalmente, es importante mencionar que los sistemas en estudio no se tratan de instituciones, sino de uno de los servicios que éstas ofrecen. Como consecuencia de lo anterior, la consideración de activos, amenazas y controles va más allá de los confinados en el contexto de una institución y por tanto incluye entidades como el usuario y sus

dispositivos o los canales de comunicación, los cuales serán tratados con mayor profundidad a pesar de no ser considerados como un bien de las instituciones financieras, debido a que éstas suelen transferir los efectos monetarios de una gran cantidad de riesgos hacia, por ejemplo, compañías aseguradoras.

## 4.3 Identificación

Retomando las descripciones generales realizadas respecto a los sistemas de banca electrónica existentes y las vulnerabilidades que éstos presentan, es pertinente ahora consolidar esta información en base a árboles analíticos.

En primer lugar se identificarán y estructurarán los activos relevantes, con la finalidad de evidenciar con mayor claridad la superficie de ataque existente. Posteriormente, se determinarán y estructurarán igualmente la diversidad de vectores de ataque hacia tales bienes.

### 4.3.1 Activos

Continuando con la clasificación y puntos de control propuestos con anterioridad, a continuación se enlistarán, estructurarán y valuarán los activos referentes a los usuarios de banca electrónica, la infraestructura que provee dichos servicios y el canal de comunicación a través del cual las transacciones son realizadas.

#### *4.3.1.1 Usuarios*

En el caso de los usuarios, sin importar si realizan banca en casa o banca a través de internet, el primer activo indispensable para acceder a los servicios es una computadora personal.

A través de este equipo, un sistema de autenticación requerirá información para verificar la identidad del usuario, por lo que las credenciales de acceso son otro activo determinante. Si tal autenticación se presenta en forma de factor único, el activo toma la forma específica de una contraseña o PIN. Si por el contrario son utilizados factores múltiples, los generadores basados en hardware o software y las tarjetas de contraseñas dinámicas deben ser considerados como credenciales adicionales (Figura 7.)

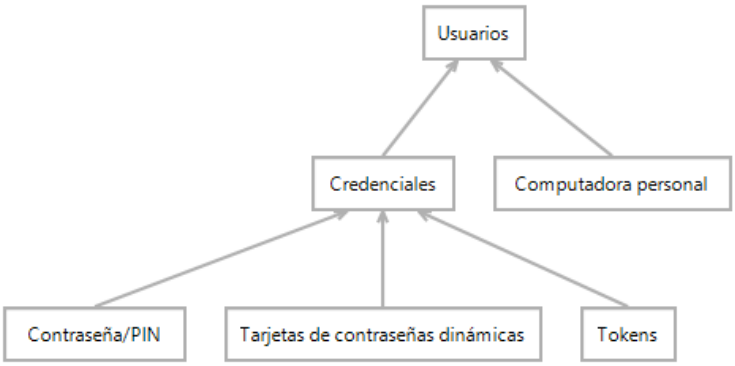


Figura 7. Listado de activos del punto de control "Usuarios."

### *4.3.1.2 Redes y servicios bancarios*

Como se mencionó anteriormente, las instituciones bancarias requieren exponer públicamente cierta zona de sus redes para el ofrecimiento de sus servicios, separando ésta de la infraestructura interna requerida para realizar operaciones ajenas a la banca electrónica.

Considerando la banca por internet, los activos más importantes serían los pertenecientes a la zona aislada de la red bancaria desde donde este servicio se ofrece, es decir, los servidores web, los sistemas bancarios que éstos consultan y los dispositivos de frontera que los protegen. Por otro lado, el día a día de las redes internas está ligado a la integridad de sus equipos y sus usuarios, debido a que los empleados bancarios pueden ser origen de ataques internos bajo coacción o soborno (Figura 8.)

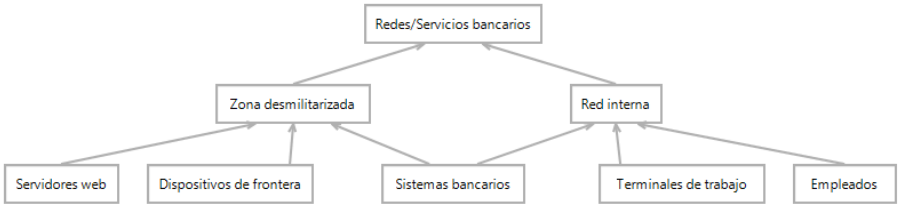


Figura 8. Listado de activos del punto de control "Redes/Servicios bancarios."

### *4.3.1.3 Canales de comunicación*

Las diferentes ofertas de banca electrónica utilizando una computadora personal estructuran su canal de comunicación seguro mediante el uso del mismo conjunto de protocolos (SSL/TLS), tanto en aplicaciones dedicadas como a través de navegadores web. Considerando lo anterior, el activo es el canal por sí mismo, variando las técnicas existentes para intentar vulnerarlo.

Incluyendo el bien anterior a los antes mencionados, el conjunto de valores identificados se concentra en el siguiente diagrama (Figura 9.)

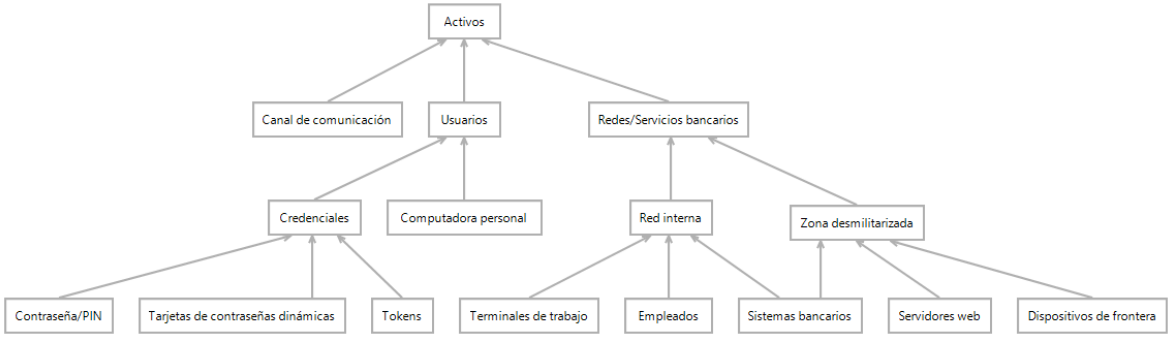


Figura 9. Listado de activos de los puntos de control en la banca electrónica mediante computadoras personales.

## 4.3.2 Amenazas

Debido a que la mayoría de las amenazas listadas en capítulos anteriores actúan sobre varias de las superficies de ataque ya identificadas, algunas de ellas aparecen en varias

categorías si se pretende clasificarlas en términos de los puntos de control propuestos, como podrá verse a continuación.

### *4.3.2.1 Hacia el usuario*

La amenaza principal hacia el primer activo antes mencionado, las credenciales de usuario, consiste en que éstas pierdan su confidencialidad de alguna manera. Por otro lado, debido a que las instituciones financieras establecen que sus cuentahabientes deben contar con un dispositivo de acceso libre de todo compromiso para la realización de transacciones, la amenaza a este activo de usuario consiste en la pérdida de ese estado óptimo.

Las métricas establecidas, a menos de que se señale de manera diferente, son el resultado de la propagación de las mismas desde los nodos hijos hacia la parte superior del árbol, siguiendo reglas específicas (Tabla 5) [32].

| Conexión | AND | OR |
|---|---|---|
| Costo | $\sum_{i=1}^{n} costo_i$ | $\frac{\sum_{i=1}^{n} prob_i x costo_i}{\sum_{i=1}^{n} prob_i}$ |
| Probabilidad | $\prod_{i=1}^{n} prob_i$ | $1 - \prod_{i=1}^{n} (1 - prob_i)$ |
| Impacto | $\frac{10^n - \prod_{i=1}^{n}(10 - impacto_i)}{10^{n-1}}$ | $\max_{i=1} impacto_i$ |

prob ∈ (0,1], costo ∈ [1, ∞), impacto ∈ [1, 10], n = número de hijos.
Tabla 5. Reglas de propagación de métricas.

Para el costo con conexión AND, es necesario que todos los nodos hijos se realicen para tener éxito, por lo que los costos se suman. Para las conexiones OR, debido a que no se tiene la certeza de qué vector de ataque se suscitará, se calcula un promedio ponderado donde el mayor peso se le da a la probabilidad.

El cálculo de probabilidades se realiza con base en los conceptos básicos de la disciplina. Para las conexiones AND se realiza el producto de la probabilidad de los eventos relacionados entre sí, mientras que en las conexiones OR se suman las probabilidades individuales de cada evento y al resultado se le sustrae la probabilidad de que ambos eventos se consoliden (Pr(A+B)=Pr(A)+Pr(B)-Pr(AB).)

El impacto para las hojas del árbol se asignó de manera discrecional (Tabla 6.) Para las conexiones OR se propaga el máximo impacto de entre los hijos, que es el peor de los casos, mientras que la idea para las conexiones AND es que el impacto del nodo padre sea mayor que el de cada uno de sus hijos, debido a que un atacante causa daño adicional conforme tiene éxito en cada uno de los nodos relacionados.

| Impacto | Descripción |
|---|---|
| Bajo (1-3) | Acción con fines legítimos o que, sin el contexto adecuado, tiene una gravedad de baja a nula por sí misma. En conjunto con otros factores puede derivar en acciones ofensivas con gravedad de baja a media. |
| Medio (4-6) | Acción abiertamente ofensiva que, sin el contexto adecuado, tiene una gravedad de baja a media por sí misma. En conjunto con otros factores puede derivar en acciones ofensivas con gravedad de media a alta. |
| Alto (7-9) | Acción abiertamente ofensiva que, sin el contexto adecuado, tiene una gravedad de media a alta por sí misma. En conjunto con otros factores puede derivar en acciones ofensivas con gravedad de alta a crítica. |
| Crítico (10) | Compromiso total |

Tabla 6. Asignación de valores de impacto.

Para la estimación del riesgo, se utilizó una fórmula que considera todas las métricas antes establecidas:

$$riesgo = \frac{prob}{costo} * impacto$$

Como se puede observar, el riesgo disminuye cuando el costo se incrementa, mientras que aumenta cuando la probabilidad y/o el impacto lo hacen también.

Con la finalidad de clarificar el valor numérico del riesgo, se puede realizar una especie de normalización utilizando la función logaritmo base 10:

$$riesgo_{norm} = \log\left(\frac{riesgo}{riesgo_{min}} * 10\right)$$

Lo anterior asignará un valor de 1 al riesgo menor y establecerá resultados más fácilmente legibles de acuerdo al comportamiento de la función utilizada.

Es importante aclarar que, para no obtener indeterminaciones en las fórmulas previas, cuando un costo es determinado como "gratuito" se considerará el valor de 1 peso al realizar los cálculos pertinentes.

**Árbol de ataque**

Objetivo: **Obtener credenciales de usuario** (Figura 10.) Costo: 8,846.35 pesos, probabilidad: 0.9971, impacto: 10, riesgo: 13.13.

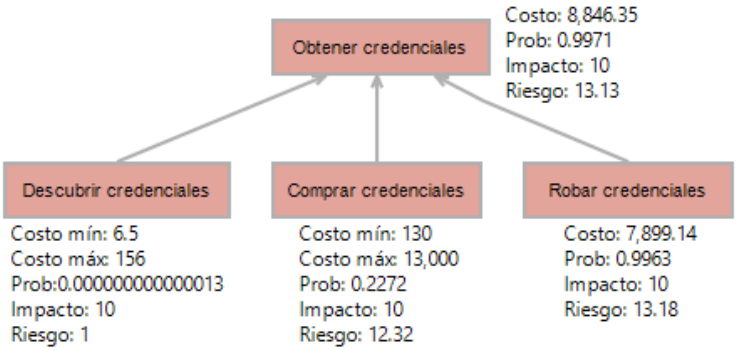


Figura 10. Árbol de ataque simplificado, cuyo objetivo es la obtención de credenciales de usuario.

Como ya se mencionó, en los diferentes sistemas de banca electrónica se utilizan dos tipos de contraseñas: una para autenticar al usuario, acceder al servicio y realizar consultas, y otra para confirmar transacciones monetarias.

1. **Descubrir credenciales mediante diccionario/fuerza bruta (consultas)** (OR, Figura 11.) Costo: entre 6.5 y 156 pesos, probabilidad de éxito: 0.000000000000013, impacto: 10, riesgo: 1.

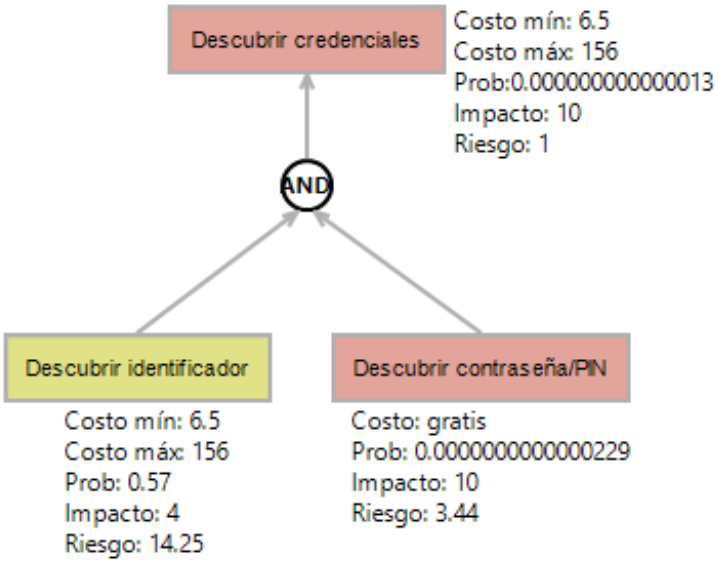


Figura 11. Especificación de la rama "Descubrir credenciales."

En la actualidad pueden adquirirse credenciales completas en el mercado negro, por lo que tendría poco sentido acudir a él para la obtención de identificadores de usuario únicamente. Sin embargo, dado que algunas ofertas de banca electrónica utilizan números de tarjeta de crédito o de cliente como identificador, algún atacante podría estar interesado en obtener este tipo de información por un costo de entre 50 centavos y 12 dólares [11]. Debido a que en México existen 21 millones de personas que cuentan con algún producto bancario y a que 12 millones ellas realizan transacciones a través de la banca electrónica de manera regular, entre 5 y 6 de cada 10 números de tarjeta o cliente adquirido contarán con servicios electrónicos:

$$Prob: \frac{Casos\ a\ favor\ del\ evento}{Casos\ posibles} = \frac{Cuentas\ con\ servicios\ electrónicos}{Cuentahabientes\ en\ México} = \frac{12\ millones}{21\ millones} = 0.57$$

Considerando los cinco bancos de mayor participación en el sector bancario mexicano [33, p. 10], el número de intentos de inicio de sesión permitidos es de 5 y, como la longitud promedio de las contraseñas utilizadas es de 8 caracteres con 62 posibilidades (a-z, A-Z, 0-9), la probabilidad de encontrar las credenciales correctas son muy limitadas, sin importar si el ataque es mediante diccionario o mediante fuerza bruta:

$$Prob: \frac{Límite\ de\ intentos}{Espacio\ de\ contraseñas} = \frac{5}{62^8} = 2.29\ x\ 10^{-14}$$

1.1 **Descubrir identificador de usuario** (AND.) Costo: entre 6.5 y 156 pesos, probabilidad de éxito: 0.57, impacto: 4, riesgo: 14.25.
1.2 **Descubrir/romper contraseña/PIN** (AND.) Costo: gratuito[52], probabilidad de éxito: 0.0000000000000229, impacto: 10, riesgo: 3.44.

Para el caso de descubrimiento de credenciales que incluyan la confirmación de transacciones, sería necesario obtener igualmente la contraseña dinámica correspondiente que, si se considera un OTP de seis caracteres numéricos (configuración muy común en los generadores comerciales), existe una probabilidad de 1 entre 1,000,000 de acertar a la contraseña correcta.

$$Prob: \frac{Número\ de\ contraseñas\ correctas}{Espacio\ de\ contraseñas\ posibles} = \frac{1}{1{,}000{,}000} = 0.000001$$

Como resultado de lo anterior, los valores de riesgo previamente establecidos crecen significativamente para este caso, sin embargo, es únicamente debido a que el riesgo mínimo de referencia (el nodo "Descubrir credenciales") disminuye también.

1.A **Descubrir credenciales mediante diccionario/fuerza bruta (transacciones)** (OR, Figura 12.) Costo: entre 6.5 y 156 pesos, probabilidad de éxito: $1.3\ x\ 10^{-20}$, impacto: 10, riesgo: 1.

1.A.1 **Descubrir identificador de usuario** (AND.) Costo: entre 6.5 y 156 pesos, probabilidad de éxito: 0.57, impacto: 4, riesgo: 20.24.
1.A.2 **Descubrir/romper contraseña/PIN** (AND.) Costo: gratuito, probabilidad de éxito: 0.0000000000000229, impacto: 10, riesgo: 9.44.
1.A.3 **Descubrir contraseña dinámica** (AND.) Costo: gratuito, probabilidad de éxito: 0.000001, impacto: 10, riesgo: 17.08.

[52] Varias de las herramientas existentes para realizar ataques de fuerza bruta o diccionario pueden obtenerse de manera gratuita en internet.

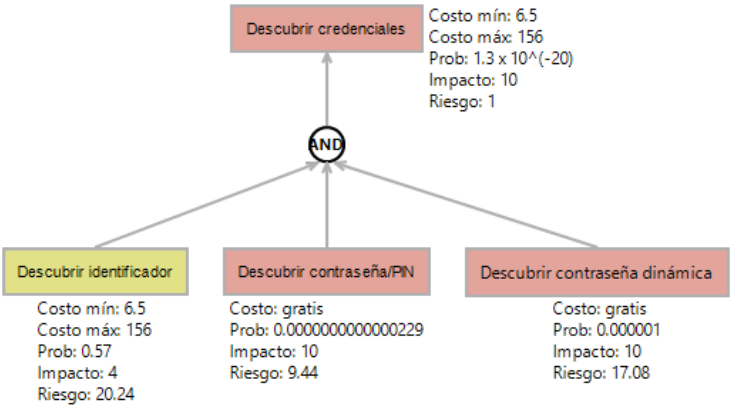


Figura 12. Especificación de la rama "Descubrir credenciales", para el caso alternativo que incluye transacciones.

A pesar de que el impacto en las métricas de esta rama es notorio, la inclusión de las contraseñas dinámicas no tiene relevancia en el objetivo general del árbol de ataque, ya que los valores del nodo raíz no sufren alteración alguna (Figura 13.)

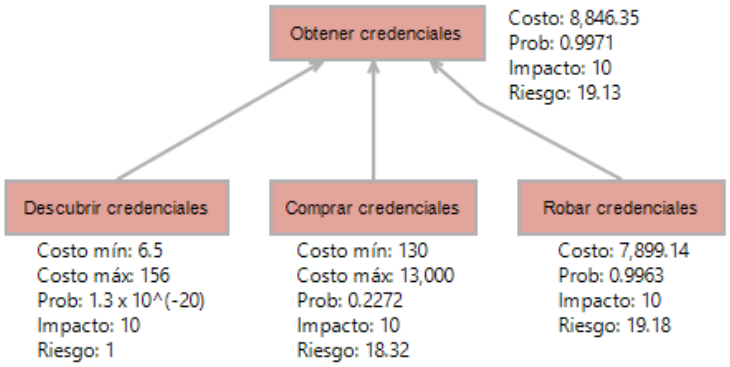


Figura 13. Árbol de ataque simplificado, cuyo objetivo es la obtención de credenciales de usuario, para el caso alternativo que incluye transacciones.

2. **Comprar credenciales** (OR, Figura 14.) Costo: entre 130 y 13,000 pesos, probabilidad: 0.2272, impacto: 10, riesgo: 12.32.

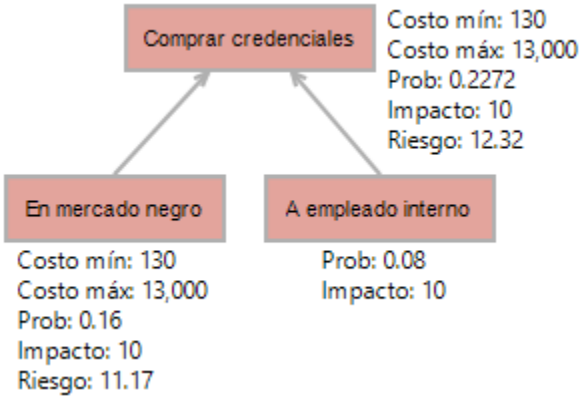


Figura 14. Especificación de la rama "Comprar credenciales."

Alrededor del 16% de las veces en las que un atacante recurre al mercado negro, lo hace para adquirir credenciales de acceso a cuentas de banca electrónica, variando el precio de éstas entre 10 y 1000 dólares, de acuerdo al saldo verificable en ellas [11].

Para el caso de filtrado de información por parte de empleados de instituciones financieras, es muy complicado establecer un costo de venta, sin embargo, si se toma en consideración el nivel de riesgo al que dicho empleado se expondría en contraste con un robo masivo (y anónimo en muchos casos) de credenciales por parte de un atacante, se podría suponer un precio superior al del mercado negro.

Una cifra que sí puede aproximarse es la probabilidad de que un banco sufra este tipo de fraude por parte de sus empleados. En el Reino Unido, por ejemplo, se observó que a lo largo del año 2012 alrededor de 8 de cada 100 fraudes cometidos de manera interna consistieron en la venta de información personal y financiera, incluyendo cuentas de banca electrónica [34]:

$$Prob: = \frac{Número\ de\ fraudes\ por\ venta\ de\ información}{Número\ de\ fraudes\ detectados} = \frac{46}{576} = 0.08$$

2.1 **Comprar en mercado negro** (OR.) Costo: entre 130 y 13,000 pesos, probabilidad: 0.16, impacto: 10, riesgo: 11.17.
2.2 **Comprar a empleado interno** (OR.) Probabilidad: 0.08, impacto: 10.

3. **Robar credenciales** (OR, Figura 15.) Costo: 7,899.14 pesos, probabilidad: 0.9963, impacto: 10, riesgo: 13.18.

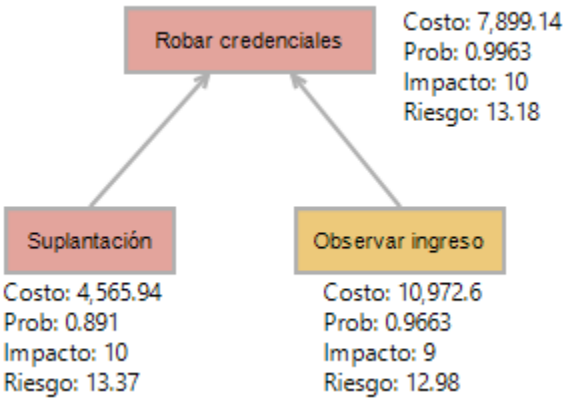


Figura 15. Especificación de la rama "Robar credenciales."

3.1 **Realizar suplantación** (OR, Figura 16.) Costo: 4,565.94 pesos, probabilidad: 0.891, impacto: 10, riesgo: 13.37.

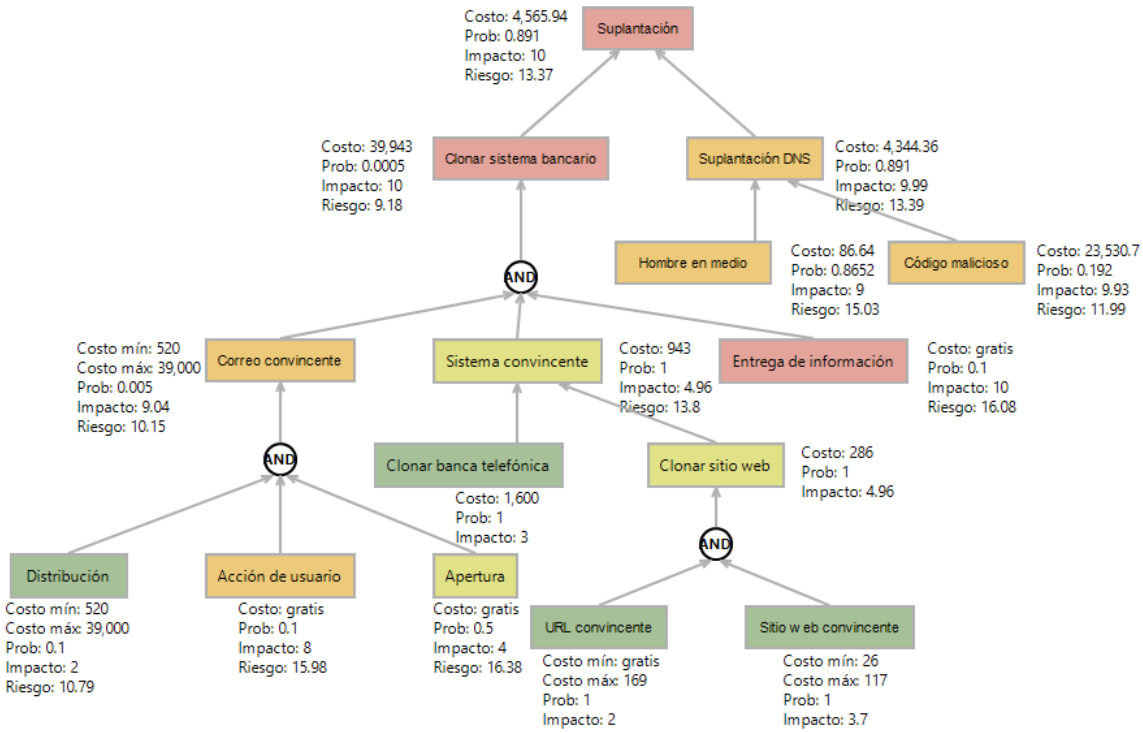


Figura 16. Especificación de la rama "Suplantación."

3.1.1 **Clonar sistema bancario** (OR.) Costo: 39,943 pesos, probabilidad: 0.0005, impacto: 10, riesgo: 9.18.

Para que la forma más común de suplantación se realice de manera exitosa se requiere en primera instancia de un correo electrónico convincente. Éstos pueden ser enviados a través de la renta del módulo de correo no deseado de una red de bots, con un costo inicial de 40 dólares[53], o adquiriendo una red de bots completa para no limitar el número de correos que pueden enviarse, por un precio entre 700 y 3000 dólares[54] [35]. Alrededor de 160 millones de correos de suplantación son enviados diariamente, de los cuales únicamente 16 millones logran pasar a través de los filtros de correo no deseado, 8 millones son abiertos y 800,000 logran que un usuario haga un clic o llame a un número telefónico [36].

$$Prob: = \frac{Número\ de\ correos\ phishing\ que\ se\ entregan}{Número\ de\ correos\ que\ se\ envían} = \frac{16\ millones}{160\ millones} = 0.1$$

$$Prob: = \frac{Número\ de\ correos\ abiertos}{Número\ de\ correos\ phishing\ que\ se\ entregan} = \frac{8\ millones}{16\ millones} = 0.5$$

$$Prob: = \frac{Número\ de\ clics\ o\ llamadas}{Número\ de\ correos\ abiertos} = \frac{800{,}000}{8\ millones} = 0.1$$

Para que el usuario entregue información después de un clic o una llamada, éste debe encontrarse con un sitio web o sistema telefónico convincente. Para el caso del sitio web,

[53] Costo por cada 20,000 correos enviados.

[54] La versión más antigua del bot ZeuS tienen un costo de 700 dólares, mientras que la más reciente alcanza hasta los 3,000 dólares.

el costo de alojamiento se encuentra entre 2 y 9 dólares mensuales[55], mientras que el registro de un dominio en algunos casos es gratuito y en otros tiene un precio adicional de hasta 13 dólares. Para el caso del sistema telefónico, uno de éstos puede duplicarse a través de un conmutador, cuyo costo inicial es de 1600 pesos[56], sin embargo, también se podría suplantar directamente a un ejecutivo bancario gratuitamente. A pesar de los esfuerzos del atacante, sólo 80,000 de las 800,000 personas que hacen clic o marcan un número telefónico caen completamente en la trampa y entregan sus credenciales.

$$Prob: = \frac{Número\ de\ entregas\ de\ credenciales}{Número\ de\ clics\ o\ llamadas} = \frac{80{,}000}{800{,}000} = 0.1$$

3.1.1.1 **Crear sistema convincente** (AND.) Costo: 943 pesos, probabilidad: 1, impacto: 4.96, riesgo: 13.8.

3.1.1.1.1 **Clonar sitio web** (OR.) Costo: 286 pesos, probabilidad: 1, impacto: 4.96.

3.1.1.1.1.1 **Crear sitio web convincente** (AND.) Costo: entre 26 y 117 pesos mensuales, probabilidad: 1, impacto: 3.7.

3.1.1.1.1.1.1 **Diseñar sitio web** (AND.) Costo: gratuito, probabilidad: 1, impacto: 3.
3.1.1.1.1.1.2 **Adquirir alojamiento en línea** (AND.) Costo: entre 26 y 117 pesos mensuales, probabilidad: 1, impacto: 1.

3.1.1.1.1.2 **Crear URL convincente** (AND.) Costo: entre gratuito y 169 pesos, probabilidad: 1, impacto: 2.

3.1.1.1.2 **Clonar banca telefónica** (OR.) Costo: 1,600, probabilidad: 1, impacto: 3.

3.1.1.2 **Enviar correo electrónico convincente** (AND.) Costo: entre 520 y 39,000 pesos, probabilidad: 0.005, impacto: 9.04, riesgo: 10.15.

3.1.1.2.1 **Distribuir correo electrónico** (AND.) Costo: entre 520 y 39,000 pesos, probabilidad: 0.1, impacto: 2, riesgo: 10.79.
3.1.1.2.2 **Apertura de correo electrónico** (AND.) Costo: gratuito, probabilidad: 0.5, impacto: 4, riesgo: 16.38.
3.1.1.2.3 **Clic o llamada por parte del usuario** (AND.) Costo: gratuito, probabilidad: 0.1, impacto: 8, riesgo: 15.98.

3.1.1.3 **Provocar entrega de información** (AND.) Costo: gratuito, probabilidad: 0.1, impacto: 8, riesgo: 15.98.

3.1.2 **Realizar suplantación DNS** (OR.) Costo: 4,344.36 pesos, probabilidad: 0.891, impacto: 9.99, riesgo: 13.39.

Una de las maneras de realizar suplantación DNS consiste en la implementación de alguna de las variaciones de hombre en medio existentes, que abren la posibilidad de modificar las respuestas de este protocolo. Un resultado similar puede obtenerse a través

[55] Límites inferior y superior en el costo de alojamiento ofrecido por las 10 mejores compañías en el ramo en Estados Unidos, de acuerdo a FindMyHosting.com.
[56] Límite inferior en el costo de "conmutadores" (2 líneas, 8 extensiones), ofrecidos en mercado libre, consultado el 14 de agosto de 2013.

de la instalación de código malicioso, que adicionalmente puede modificar archivos host y hasta establecer proxys en sistema operativo o navegadores web.

Considerando el primer caso, una opción es utilizar un nodo TOR de salida malicioso que, debido a ser el único punto en donde la información viaja en claro, es ideal para espiar y modificar información. En el año 2012, un promedio de 2918 nodos TOR se encontraron activos, de los cuales 902 eran nodos de salida y 8 de ellos reportaron tráfico malicioso [37].

$$Prob: = \frac{Número\ de\ nodos\ maliciosos}{Número\ de\ nodos\ de\ salida} = \frac{8}{902} = 0.0088$$

Cabe mencionar que el número de usuarios de TOR a nivel mundial es de aproximadamente 1,200,000 [38], que es una cantidad muy baja. Sin embargo, esta métrica está referida a la probabilidad de ser víctima de un ataque de hombre en medio una vez que se ha decidido acceder a esta red.

Otra alternativa es la creación de un punto de acceso inalámbrico malicioso. Las características de algunas computadoras permiten la configuración de éstas como puntos de acceso, sin embargo, un repetidor con alcance de 500 metros puede adquirirse desde 450 pesos[57]. En cuanto a su frecuencia, algunos estudios afirman que al menos 20% de las corporaciones de todo tipo han tenido un punto de acceso malicioso dentro del alcance de su red inalámbrica en al menos una ocasión [39].

Finalmente, se encuentra la opción de realizar envenenamiento del protocolo ARP dentro de una red local y monitorear el tráfico que pasa por ella. El 83% de las redes son vulnerables a este tipo de ataque [40].

3.1.2.1 **Realizar hombre en medio** (OR, Figura 17.) Costo: 86.64 pesos, probabilidad: 0.8652, impacto: 9, riesgo: 15.03.

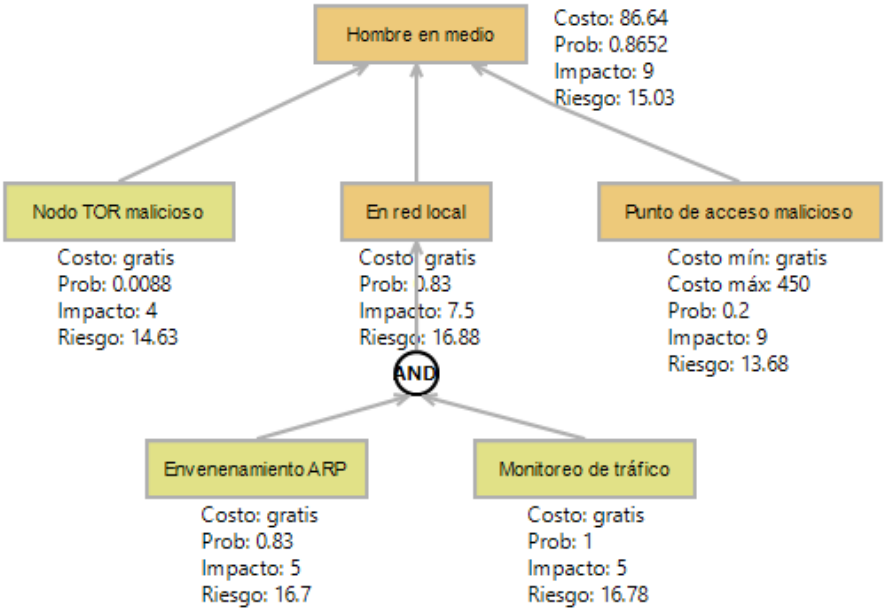


Figura 17. Especificación de la rama "Hombre en medio."

[57] En mercado libre, ofrecidos por vendedores con mayor reputación, consultado el 14 de agosto de 2013.

3.1.2.1.1 **Crear nodo TOR malicioso** (OR.) Costo: gratuito, probabilidad: 0.0088, impacto: 4, riesgo: 14.63.

3.1.2.1.2 **Crear punto de acceso malicioso** (OR.) Costo: entre gratuito y 450 pesos, probabilidad: 0.2, impacto: 9, riesgo: 13.68.

3.1.2.1.3 **Realizar hombre en medio en red local** (OR.) Costo: gratuito, probabilidad: 0.83, impacto: 7.5, riesgo: 16.88.

3.1.2.1.3.1 **Realizar envenenamiento ARP** (AND.) Costo: gratuito, probabilidad: 0.83, impacto: 5, riesgo: 16.7.

3.1.2.1.3.2 **Realizar monitoreo de tráfico** (AND.) Costo: gratuito, probabilidad: 1, impacto: 5, riesgo: 16.78.

3.1.2.2 **Instalar código malicioso en dispositivo de usuario** (OR, Figura 18.) Costo: 23,530.7, probabilidad: 0.192, impacto: 9.93, riesgo: 11.99.

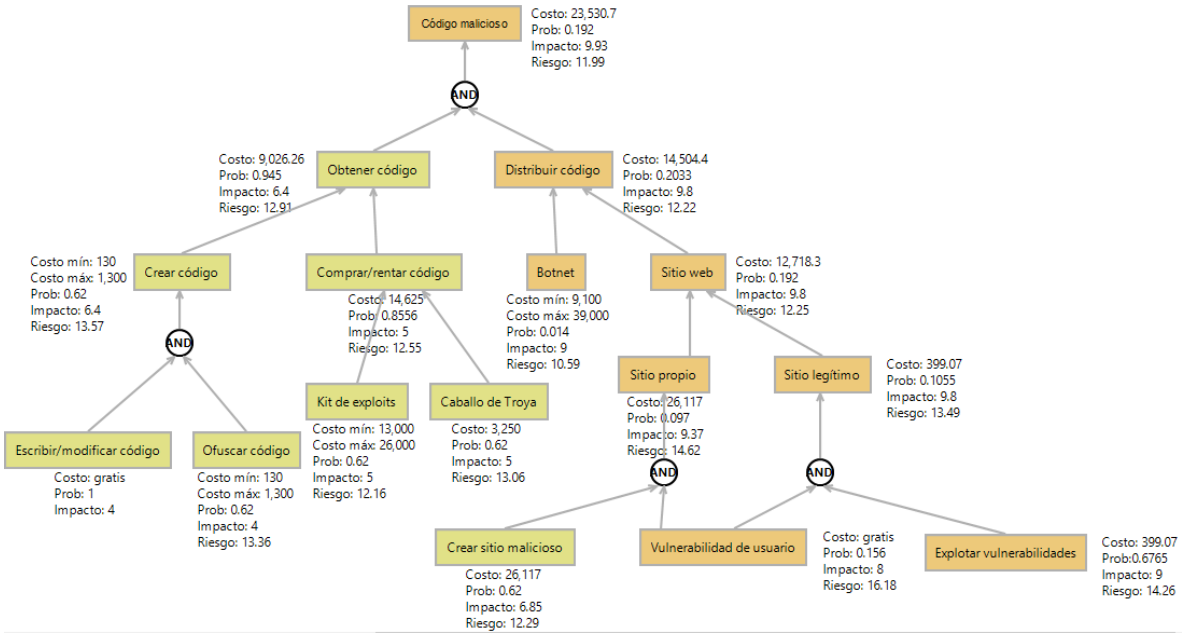


Figura 18. Especificación de la rama "Código malicioso."

La obtención de código malicioso puede realizarse mediante creación original o modificación de algún código existente, o adquiriéndolo en el mercado negro. Estudios han demostrado que las soluciones antivirus cuentan con un nivel de detección no mayor a 38% para códigos de día cero [41], debido en muchas ocasiones a la ausencia de firmas y a la ofuscación con la que esta clase de amenazas son creadas. Las herramientas para dificultar la detección pueden ser adquiridas por un costo de entre 10 y 1000 dólares [35].

Si en lugar de crear/modificar y ofuscar se desea adquirir código malicioso ya desarrollado, en el mercado negro pueden encontrarse artículos como caballos de Troya[58] por 250 dólares o juegos de exploits para creación de sitios web maliciosos en el rango de 1000 y 2000 dólares [35], muchos de ellos con la posibilidad de explotar vulnerabilidades día cero, igualmente.

[58] Caballos de Troya para acceso remoto, como lo son Gh0st Rat, Poison Ivy o Turkojan.

3.1.2.2.1 **Obtener código malicioso** (AND.) Costo: 9,026.26 pesos, probabilidad: 0.945, impacto: 6.4, riesgo: 12.91.

3.1.2.2.1.1 **Crear código malicioso** (OR.) Costo: entre 130 y 1,300 pesos, probabilidad: 0.62, impacto: 6.4, riesgo: 13.57.

3.1.2.2.1.1.1 **Escribir/modificar código malicioso** (AND.) Costo: gratuito, probabilidad: 1, impacto: 4.

3.1.2.2.1.1.2 **Ofuscar código malicioso** (AND.) Costo: entre 130 y 1,300 pesos, probabilidad: 0.62, impacto: 4, riesgo: 13.36.

3.1.2.2.1.2 **Comprar/rentar código malicioso** (OR.) Costo: 14,625 pesos, probabilidad: 0.8556, impacto: 5, riesgo: 12.55.

3.1.2.2.1.2.1 **Caballos de Troya** (OR.) Costo: 3,250 pesos, probabilidad: 0.62, impacto: 5, riesgo: 13.06.

3.1.2.2.1.2.2 **Kit de exploits** (OR.) Costo: entre 13,000 y 26,000 pesos, probabilidad: 0.62, impacto: 5, riesgo: 12.16.

3.1.2.2.2 **Distribuir código malicioso** (AND.) Costo: 14,504.4, probabilidad: 0.2033, impacto: 9.8, riesgo: 12.22.

Algunos de los medios de distribución de código malicioso más populares involucran la persuasión del usuario a través de ingeniería social para que éste visite o sea direccionado hacia un sitio web o realice la apertura de un archivo adjunto a un correo electrónico, además del envío a través de una red de bots cuando un equipo ya se encuentra comprometido.

Para el caso de distribución vía web, existe la opción de crear un sitio malicioso desde cero o de comprometer un sitio legítimo. En ambos casos, es necesario en primera instancia que el equipo del usuario visitante sea vulnerable de alguna forma: en el año 2012, de 10,541,379 usuarios expuestos a un sitio web malicioso con exploits dedicados al complemento de java para firefox, 5,356,074 utilizaban ese navegador, 3,909,934 tenían instalado dicho complemento y 1,642,172 tenían instalada una versión vulnerable del mismo [42].

$$Prob: = \frac{Número\ de\ usuarios\ vulnerables}{Número\ de\ usuarios\ expuestos} = \frac{1{,}642{,}172}{10{,}541{,}379} = 0.156$$

Considerando ahora la posibilidad de inyectar código malicioso en un sitio legítimo, se deben incluir las posibles vulnerabilidades del sitio en cuestión. En 2012, la probabilidad de que una página contara con al menos una vulnerabilidad seria explotable mediante secuencias de comandos en sitios cruzados fue de 0.53, mediante falsificación de peticiones en sitios cruzados de 0.26 y mediante algún tipo de inyección de 0.07 [43].

Una manera de identificar estas debilidades, si no se desea hacerlo a mano, es mediante la adquisición en el mercado negro de escáneres de vulnerabilidad a secuencias de comandos en sitios cruzados[59] por entre 10 y 30 dólares, o de herramientas para inyección SQL por entre 15 y 150 dólares, por citar algunos ejemplos [11].

[59] En algunos casos el escáner es también capaz de realizar exploit.

Finalmente, para el caso de redes de bots, de entre los casi 904 millones de computadoras con conexión a internet existentes a nivel mundial en el año 2012 [44], se cree que alrededor de 13 millones de ellas se encontraban infectadas por alguna variante del bot ZeuS [45], posibilitando la instalación de una mayor cantidad de código malicioso con fines delictivos de diversa índole.

$$Prob: = \frac{Número\ de\ equipos\ infectados}{Número\ de\ equipos\ con\ conexión\ a\ internet} = \frac{13\ millones}{904\ millones} = 0.14$$

3.1.2.2.2.1 **Comprar bot** (OR.) Costo: entre 9,100 y 39,000 pesos, probabilidad: 0.014, impacto: 9, riesgo: 10.59.

3.1.2.2.2.2 **Vía web** (OR.) Costo: 12,718.3, probabilidad: 0.192, impacto: 9.8, riesgo: 12.22.

3.1.2.2.2.2.1 **A través de un sitio propio** (OR.) Costo: 26,117 pesos, probabilidad: 0.097, impacto: 9.37, riesgo: 14.62.

3.1.2.2.2.2.1.1 **Crear sitio web malicioso** (AND.) Costo: 26,117 pesos, probabilidad: 0.62, impacto: 6.85, riesgo: 12.29.

3.1.2.2.2.2.1.1.1 **Crear sitio web convincente** (ataque 3.1.1.1.1.1, AND.)

3.1.2.2.2.2.1.1.2 **Kit de exploits** (ataque 3.1.2.2.1.2.2, AND.)

3.1.2.2.2.2.1.2 **Explotar vulnerabilidad de usuario** (AND.) Costo: gratuito, probabilidad: 0.156, impacto: 8, riesgo: 16.18.

3.1.2.2.2.2.2 **A través de un sitio legítimo** (OR.) Costo: 399.07 pesos, probabilidad: 0.1055, impacto: 9.8, riesgo: 12.25.

3.1.2.2.2.2.2.1 **Explotar vulnerabilidades de servidores/aplicaciones web** (OR, Figura 19) Costo: 399.07 pesos, probabilidad: 0.6765, impacto: 9, riesgo: 14.26.

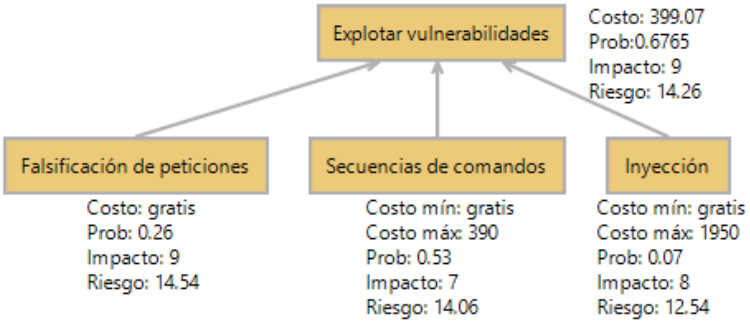


Figura 19. Especificación de la rama "Explotar vulnerabilidades."

3.1.2.2.2.2.1.1.1 **Realizar inyección** (OR.) Costo: entre gratuito y 1950 pesos, probabilidad: 0.07, impacto: 8, riesgo: 12.54.

3.1.2.2.2.2.1.1.2 **Realizar secuencias de comandos en sitios cruzados** (OR.) Costo: entre gratuito y 390 pesos, probabilidad: 0.53, impacto: 7, riesgo: 14.06.

3.1.2.2.2.2.1.1.3 **Realizar falsificación de peticiones en sitios cruzados** (OR.) Costo: gratuito, probabilidad: 0.26, impacto: 9, riesgo: 14.54.

Retomando la diferenciación entre transacción y consulta, mencionada al inicio del análisis, es importante mencionar que todos los ataques derivados en la rama "Robo de credenciales" tienen la posibilidad de incluir las contraseñas dinámicas entre sus objetivos, por lo que en este caso no es necesario establecer árboles alternativos.

3.2 **Observar ingreso de credenciales** (OR, Figura 20.) Costo: 10,972.6 pesos, probabilidad: 0.9663, impacto: 9, riesgo: 12.98.

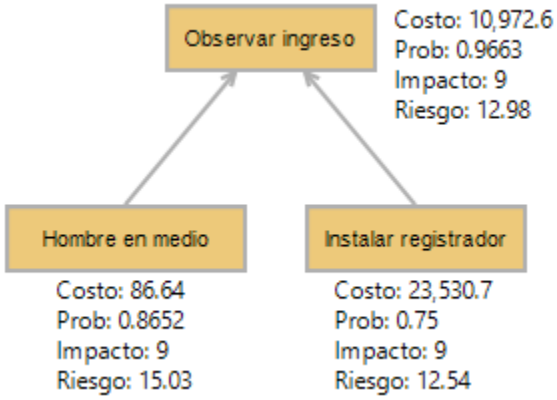


Figura 20. Especificación de la rama "Observar ingreso."

3.2.1 **Realizar hombre en medio** (ataque 3.1.2.1, OR.)

En 2012, se consideró que de entre todas las posibles formas que el código malicioso puede tomar, en el 75% de las ocasiones tal forma incluye la presencia de un registrador de teclas o de ratón [46].

3.2.2 **Instalar registrador** (OR.) Costo: 23,530.7 pesos, probabilidad: 0.75, impacto: 9, riesgo: 12.54.

### *4.3.2.2 Hacia el canal de comunicación*

En lo referente al canal de comunicación, la principal amenaza consiste en que el medio de transmisión pierda su carácter de "seguro", hecho que permitiría desde la pérdida de confidencialidad de los datos utilizados en las transacciones, hasta la modificación de los mismos en beneficio de los atacantes.

Objetivo: **Comprometer las comunicaciones**.

1.1.1 **Capturar/alterar comunicaciones** (OR, Figura 21.) Costo: 4,344.36 pesos, probabilidad: 0.891, impacto: 9.99, riesgo: 13.39.

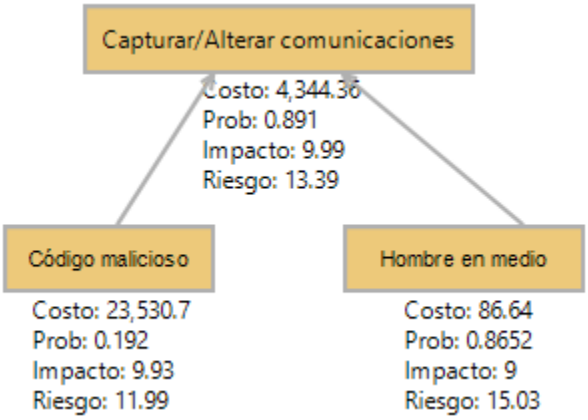


Figura 21. Especificación de la rama "Capturar/Alterar comunicaciones."

1.2 **Realizar hombre en medio** (ataque 3.1.2.1, OR.)
1.3 **Instalar código malicioso en dispositivo de usuario** (ataque 3.1.2.2, OR.)

### *4.3.2.3 Hacia las redes y servicios bancarios*

Las amenazas concernientes a las zonas desmilitarizadas están asociadas a las vulnerabilidades de los elementos presentes en ellas. En el caso de cortafuegos, debe considerarse la posibilidad de que éstos no realicen correctamente su función o que dejen de operar por completo.

En cuanto a servidores web, la problemática se centra tanto en vulnerabilidades en el software utilizado para proveer el servicio, en errores de configuración y validación de datos de entrada o salida, como en la amenaza cada vez más presente de ataques de denegación de servicio a través de redes de bots o planificación de colectivos.

Tomando en cuenta ahora la parte no expuesta de los servicios bancarios, las principales preocupaciones radican en la integridad de tales redes y de la información que circula en ellas día a día. El compromiso en estos activos puede originarse mediante la instalación de código malicioso (por ataques tanto externos como internos) en algún elemento de la infraestructura o debido a la filtración de información sensible por parte de empleados.

Objetivo: **Comprometer las redes y servicios bancarios**.

2. **Ataque externo** (OR.)

2.1 **Atacar cortafuegos** (OR.)

2.1.1 **Provocar denegación de servicio** (OR.)

2.1.1.1 **Explotar errores de configuración** (OR.)
2.1.1.2 **Explotar vulnerabilidades de dispositivos específicos** (OR.)
2.1.1.3 **Provocar denegación de servicio distribuida** (OR.)

2.1.1.3.1 **Rentar una red de bots** (OR.) Costo: desde 6955 pesos[60] [35].

[60] El costo de rentar una botnet para realizar un ataque de DDoS durante 1 semana, 5 horas al día, es de 535 dólares.

2.1.1.3.2 **Comprar red de bots** (Ataque 3.1.2.2.2.1, OR.)
2.1.1.3.3 **Utilizar planificación de colectivos** (OR.) Costo: gratuito.

2.1.2 **Evadir reglas de filtrado** (OR.)

2.1.2.1 **Explotar errores de configuración** (ataque 4.1.1.1, OR.)
2.1.2.2 **Explotar vulnerabilidades de dispositivos específicos** (ataque 4.1.1.2, OR.)

2.2 **Atacar servidores/aplicaciones web** (OR.)

2.2.1 **Robar información de usuarios** (OR.)

2.2.1.1 **Explotar vulnerabilidades de servidores/aplicaciones web** (ataque 3.1.2.2.2.2.1, OR.)

2.2.2 **Provocar denegación de servicio** (OR.)

2.2.2.1 **Provocar denegación de servicio distribuida** (ataque 4.1.1.3, OR.)
2.2.2.2 **Explotar vulnerabilidades de servidores/aplicaciones web** (ataque 3.1.2.2.2.2.1, OR.)

3. **Ataque interno** (OR.)

3.1 **Atacar sistemas bancarios/terminales de trabajo** (OR.)

3.1.1 **Instalar código malicioso en dispositivo de usuario** (Ataque 3.1.2.2, OR.)

3.2 **Provocar divulgación de información por parte de empleado** (OR.)

3.2.1 **Sobornar a empleado** (OR.)
3.2.2 **Amenazar a empleado** (OR.)

En el análisis anterior puede observarse una gran variación en los costos de realización de los diferentes ataques, sin embargo, es importante hacer varios comentarios al respecto.

En base a aspectos únicamente económicos, la opción más atractiva parece ser el descubrimiento de credenciales a través de ataques de diccionario o fuerza bruta, sin embargo, además de que la inversión realizada es muy poco amortizable (dependiendo de la longitud y tipo de caracteres utilizados, una contraseña puede demorar una gran cantidad de tiempo en ser descubierta o no ser encontrada jamás en última instancia), este tipo de ataque puede ser fácilmente mitigado mediante la utilización de dos factores de autenticación o la limitación de intentos de inicio de sesión, característica que se ve reflejada en su valor de probabilidad.

Por otro lado, a través de la compra de credenciales de usuario a un empleado o en el mercado negro, suponiendo que sean auténticas, se tiene acceso únicamente a la cuenta cuya información se posee, limitando las ganancias al contenido encontrado en ella y limitando igualmente la amortización del ataque.

Finalmente, el robo de credenciales cuenta con propiedades muy interesantes a pesar de ser potencialmente la más costosa. El peor de los casos para el atacante, en términos de inversión a realizar, resulta ser la adquisición de una red de bots, sin embargo, sus múltiples funcionalidades (captura de credenciales, captura de certificados digitales, captura de

galletas informáticas, servidor proxy, registrador, modificación de archivos host, correo no deseado, denegación de servicio distribuida, distribución de código malicioso, entre otras) hacen posible la distribución del costo total entre todos los vectores de ataque que son cubiertos, haciéndolos más baratos.

Por otro lado, la relación costo beneficio que puede obtenerse es realmente significativa. En el año 2012, una variación del bot ZeuS obtuvo acceso a la información bancaria de cerca de 30,000 cuentahabientes de instituciones financieras italianas, alemanas, españolas y holandesas, lo que derivó en el robo de entre 500 y 250,000 euros por usuario y en la pérdida total de 36 millones [47]. Aunque los responsables se mantuvieran en el límite inferior de dinero sustraído a cada cuenta, sólo serían requeridos cinco ataques exitosos para recuperar la inversión realizada, haciendo de este vector de ataque uno de los más rentables.

Considerando ahora cuestiones de probabilidad y riesgo, el robo de credenciales de usuario junto con la captura y alteración de las comunicaciones resultan ser los que mayor probabilidad de ocurrencia presentan. Además de que cuentan con un valor de riesgo similar, tienen en común que el vector de hombre en medio, específicamente su modalidad en redes locales cableadas o inalámbricas, es el que presenta la combinación de costo, probabilidad e impacto más favorable para un atacante.

Siendo así, los resultados parecen indicar que aún hoy, el principal riesgo para la realización de banca electrónica es llevarla a cabo en una red local pública, donde el usuario puede ser víctima de un ataque de hombre en medio que derive en la alteración directa de transacciones o en un ataque de suplantación de identidad que provoque la entrega de información sensible de manera involuntaria e inadvertida.

## 4.4 Evaluación

Una vez identificados los principales vectores de ataque a los que se encuentran expuestos los servicios de banca electrónica, se puede proceder a una evaluación inicial de las medidas adoptadas por los cinco principales bancos que operan en México [33], como conjunto, confrontándolas directamente con el árbol de ataque genérico antes estructurado.

### 4.4.1 Rama “Descubrir credenciales”

El proceso inicial de autenticación requiere, salvo una excepción en la que se utiliza el número de cliente, de un identificador de usuario alfanumérico de al menos seis caracteres y una contraseña de acceso igualmente alfanumérica para todos los casos, en cumplimiento con las regulaciones mexicanas. Adicionalmente es utilizada una segunda contraseña para confirmar la realización de transacciones, la cual puede ser estática (pero diferente a la establecida para acceder al servicio) o dinámica.

La obtención de estas contraseñas de un sólo uso puede llevarse a cabo mediante tablas de contraseñas dinámicas o mediante generadores que, excluyendo un ejemplo que utiliza el esquema de reto/respuesta y otro que ofrece un generador en forma de aplicación móvil, están basados en tiempo.

El requerimiento de los segundos factores de autenticación, en conjunto con el límite de intentos de inicio de sesión y consecuente bloqueo de credenciales mencionados anteriormente, mitigan de manera suficientemente efectiva el riesgo de que las

credenciales de usuario sean descubiertas, ya que aunque se conozca un identificador de usuario, la probabilidad de adivinar o romper una contraseña de acceso o transacción es extremadamente baja (Figura 22.)

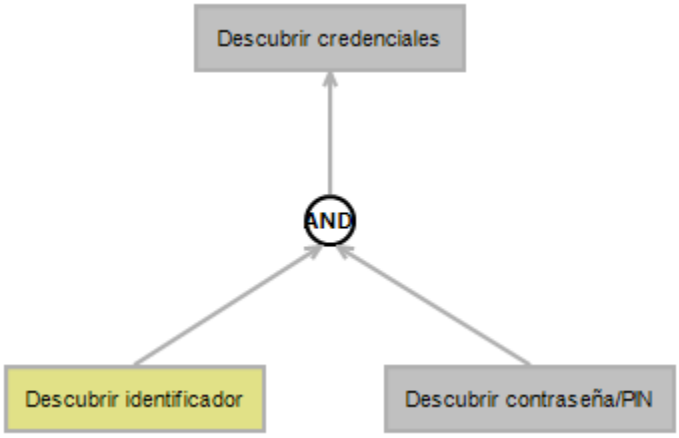


Figura 22. Nodos mitigados por controles (gris) en la rama "Descubrir credenciales."

### 4.4.2 Rama "Comprar credenciales"

La CNVB, en el artículo 316 de la Circular Única de Bancos, establece que las instituciones tienen prohibido contar con cualquier mecanismo que les permita recuperar la información de autenticación de sus cuentahabientes, además de que un empleado bancario igualmente no tiene permitido solicitar este tipo de información a un usuario. Para fortalecer la regulación en este sentido, cada banco suele establecer políticas y sanciones internas para prevenir todo tipo de fraude, además de cursos mandatorios para todo su personal.

Lo acciones anteriores ayudan a que los fraudes a través de filtrado de información se susciten con menor frecuencia, sin embargo, el comercio de credenciales en el mercado negro sigue siendo una actividad muy lucrativa, por lo que se puede considerar que el riesgo asociado a esta rama no se encuentra suficientemente mitigado (Figura 23.)

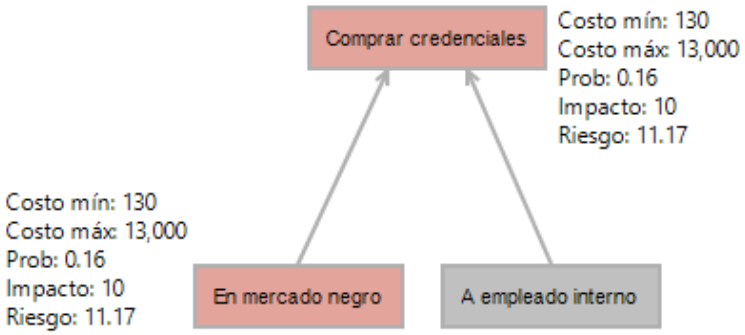


Figura 23. Nodos mitigados por controles (gris) en la rama "Comprar credenciales."

### 4.4.3 Rama "Robar credenciales"

El primer control en este sentido es el establecimiento de un canal de comunicación seguro entre el cliente y el sistema bancario a través del protocolo SSL. Parar lograr lo

anterior, en todos los casos estudiados se cuenta con un esquema de llave pública cuya dimensión es 128 bits.

Esta medida no ofrece protección contra suplantación, algunos tipos de hombre en medio o registro de teclas y, si el equipo desde el que se realizan transacciones ya se encuentra comprometido con algún tipo de código malicioso, el canal de comunicación seguro es completamente inservible.

Con la finalidad de evitar el compromiso de los equipos de los cuentahabientes, algunas instituciones han adoptado el uso de herramientas de terceros que pretenden proteger de una amplia gama de ataques, como lo son Rapport y Ahnlab Online Security (AOS).

Rapport está diseñado para proteger información confidencial en una transacción a través de internet mediante el establecimiento de medidas contra la suplantación, contra hombre en medio, contra el registro de teclas y contra código malicioso [48].

Esta herramienta ha tenido una gran publicidad a nivel mundial y varias instituciones financieras (dos, en el caso mexicano) la han adoptado como parte de las medidas de protección que sus sistemas de banca electrónica ofrecen, sin embargo, en el último par de años se han generado muchas críticas tanto por la cantidad de recursos necesarios para su ejecución (al grado de llegar a provocar denegación de servicio en algunos equipos Windows), como por vulnerabilidades descubiertas que inutilizan varios de sus módulos.

En 2010, se demostró que el mecanismo utilizado entonces para proteger al usuario del registro de teclas, un driver adicional para el teclado del equipo que cifraba la información de las teclas oprimidas, podía ser vulnerado de manera casi trivial debido al débil algoritmo utilizado (cifrado por sustitución) y al pobre manejo de las llaves secretas [49]. El desarrollador argumentó que, debido a que debían cumplirse ciertos escenarios específicos para que esta amenaza se consolidara, el riesgo para sus usuarios era mínimo. Posteriormente liberó un parche que pretendía mitigar esta vulnerabilidad, aunque sus críticos no consideraron que lo hiciera efectivamente [50].

Otra vulnerabilidad, descubierta en 2013 para la versión 1208.41 y anteriores, permite anular la autoevaluación y el sistema de intercepción de la herramienta, que son las bases de su módulo protector contra código malicioso. De manera similar, el desarrollador minimizó la amenaza y, al menos hasta el mes de Agosto, se encontraba en proceso de liberar un parche [51].

Aunado a lo anterior, también en 2013, una variante del bot ZeuS que se hace pasar por una actualización de Rapport ha comenzado a circular por la red [52].

De manera similar, otra herramienta diseñada para proteger al usuario que no ha alcanzado los niveles de popularidad de Rapport (en el caso mexicano, sólo una institución la incluye dentro de sus medidas de protección), es AOS. Dentro de sus principales características se incluyen medidas contra registro de teclas y captura de pantalla, contra el código malicioso residente en memoria RAM, la revisión del estado de actualizaciones del sistema operativo huésped [53], así como la implementación de un cortafuegos y navegador web propios de la herramienta [54].

Aunque no se han reportado vulnerabilidades de manera tan frecuente como con Rapport, entre 2008 y 2012 se identificaron al menos nueve errores (la mayoría con un nivel

de criticidad de medio a bajo) relacionados con la capacidad de la herramienta de detectar código malicioso [55].

Considerando los casos mencionados y el tipo de servicios que este tipo de herramientas busca proteger, es de esperar que continúen saliendo a la luz vulnerabilidades con diferentes grados de criticidad. Adicionalmente, sólo tres de los cinco servicios de banca electrónica analizados implementan esta clase de medidas, por lo que se podría considerar de manera general que las ramas referentes a suplantación, hombre en medio, registro de teclas y código malicioso, no se encuentran totalmente mitigadas.

Una última medida que las instituciones financieras establecen para proteger a sus cuentahabientes es el estudio de sus hábitos de consumo, combinado con notificaciones de movimientos vía mensajes a teléfonos móviles y correo electrónico o llamadas telefónicas. Tales notificaciones pueden ser resultado de alguna actividad sospechosa o una notificación basada en los montos para transacciones que un usuario puede delimitar de manera previa. En cualquiera de los casos, estas alertas generalmente tienen la finalidad de verificar la legitimidad de la transacción identificada.

#### *4.4.3.1 Educación y buenas prácticas*

Muchos de los ataques a los que los sistemas de banca electrónica se encuentran expuestos son producto de malas decisiones de sus usuarios y, a su vez, la colaboración de los mismos es un gran paso para lograr menores incidentes de seguridad en las transacciones en línea.

Debido a lo anterior y a que las regulaciones mexicanas así lo establecen, los portales bancarios incluyen secciones con descripciones de los riesgos inherentes a las actividades financieras por medios electrónicos, así como sugerencias y buenas prácticas seguridad para mitigarlos.

La importancia de estas actividades de educación puede ser claramente observada al contextualizar, en el árbol de ataque previamente estructurado, un caso hipotético en el que todo usuario tuviera siempre presente las recomendaciones y buenas prácticas de seguridad al tomar decisiones en un entorno de transacciones en línea:

En el referente a suplantación mediante la clonación de un sitio web bancario, aún cuando un correo fraudulento lograra evadir los filtros correspondientes y el usuario lo abriera, éste contaría con la información y criterios suficientes para sospechar del mensaje recibido, no hacer clic en la liga incluida y mucho menos ingresar información sensible, aún cuando la página destino fuera altamente convincente (Figura 24.)

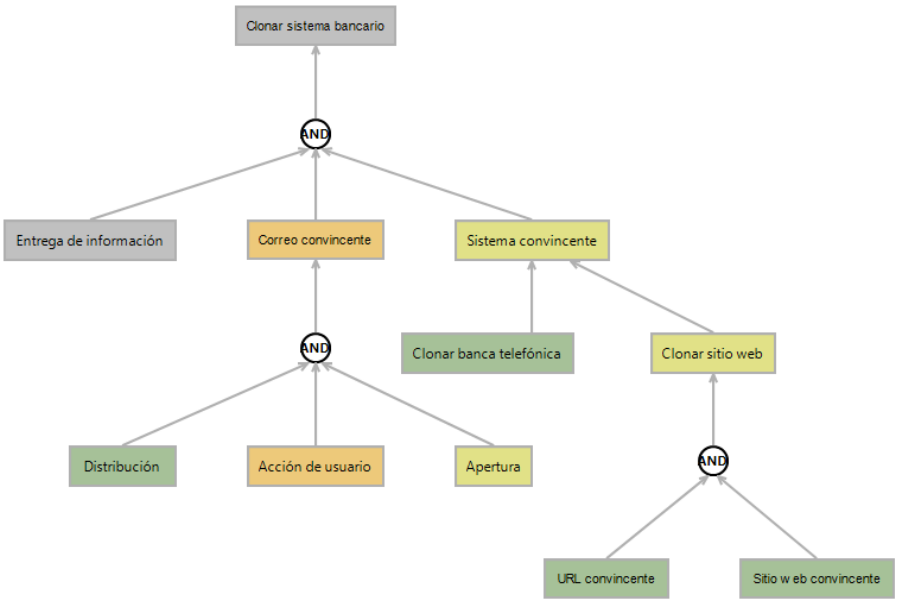


Figura 24. Nodos mitigados por controles (gris) en la rama "Clonar sistema bancario."

Por otro lado, en el caso de código malicioso utilizado en la modificación de respuestas DNS y de comunicaciones, aún cuando ha sido establecido que las soluciones comerciales no son efectivas contra la totalidad de código malicioso existente, su distribución a través de sitios web maliciosos o legítimos podría ser prevenida al no existir vulnerabilidades en el equipo del usuario, ya que éste conocería la importancia de mantener actualizados sistemas operativos, aplicaciones y complementos (Figura 25.)

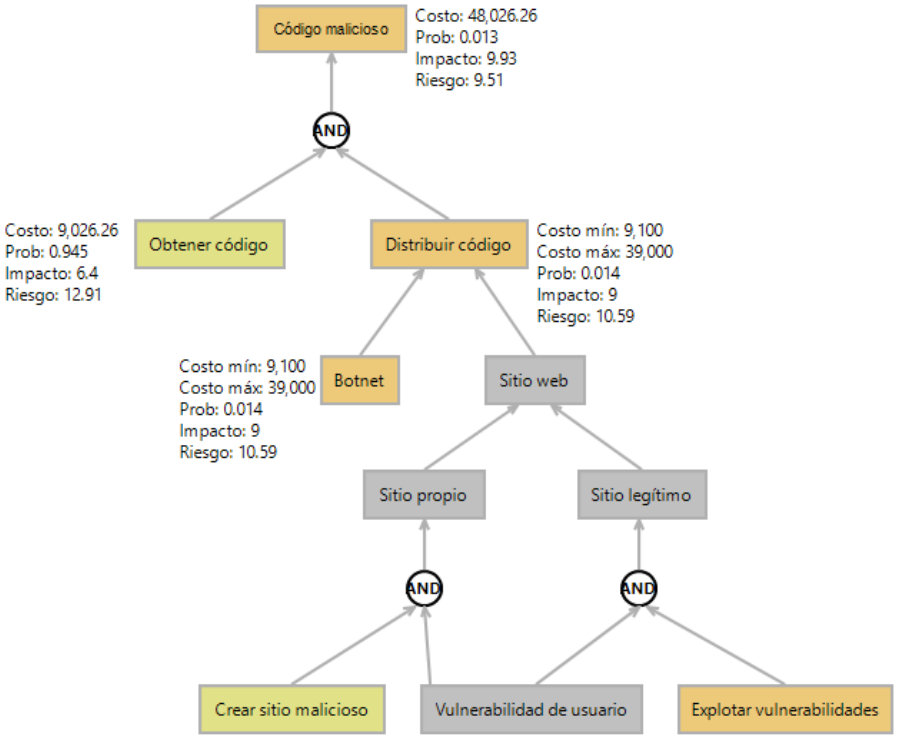


Figura 25. Nodos mitigados por controles (gris) en la rama "Código malicioso."

Finalmente, para el caso de hombre en medio, las actividades de concientización reducirían en gran medida el riesgo de dos de los principales vectores de ataque en esta clasificación, debido a que a los usuarios serían más cuidadosos en lo referente a la red pública a la que se conectan y al tipo de transacciones que realizarían en ésta, aún cuando fuera legítima (Figura 26.)

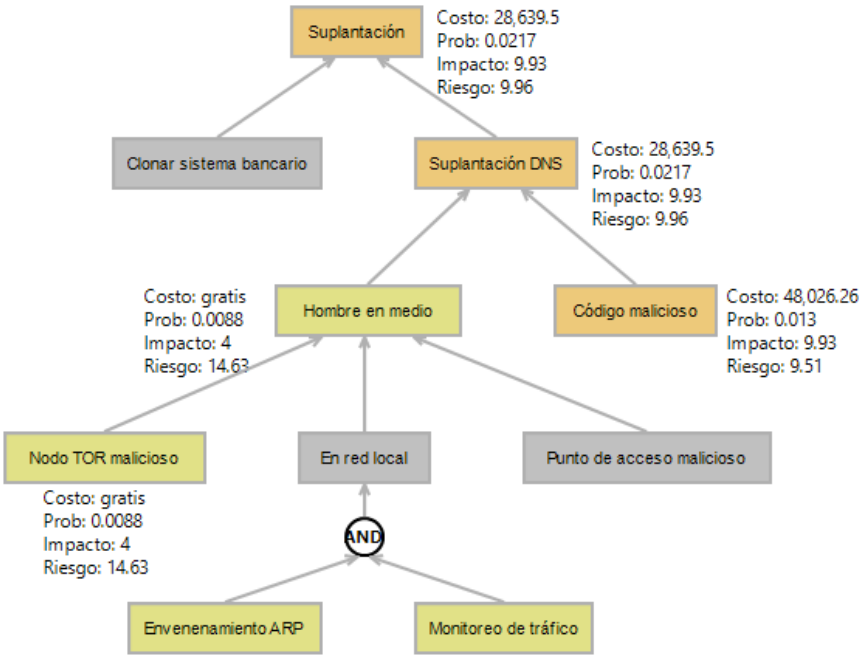


Figura 26. Nodos mitigados por controles (gris) en la rama "Suplantación."

Fuera del ámbito hipotético, algunos efectos de esta labor de difusión son igualmente visibles: en 2012, el 71% de los internautas consideraron que la responsabilidad de salvaguardar la seguridad en la banca por internet recaía tanto en el banco como en ellos mismos, contrastando con el 27% que asume que la institución debe ser la única encargada, cifra que es un 4% menor a la recabada en 2011 [2]. Adicionalmente, algunas instituciones señalan que en los últimos años el nivel de fraude que han experimentado es muy bajo, siendo el monto de pérdidas de alrededor de cien mil pesos al mes [56].

Las consecuencias de las medidas de protección descritas, tanto desde la perspectiva técnica como de regulación y concientización hipotética, pueden observarse en algunas reducciones en los valores de probabilidad y riesgo de varios nodos que, al propagarse a la parte superior del árbol, resultan en la disminución de casi 20% en la probabilidad de vulneración de transacciones en general, de casi 0.9 puntos de su riesgo asociado y, así mismo, se presenta un aumento de más de 500% en los costos de realización (Figura 27.)

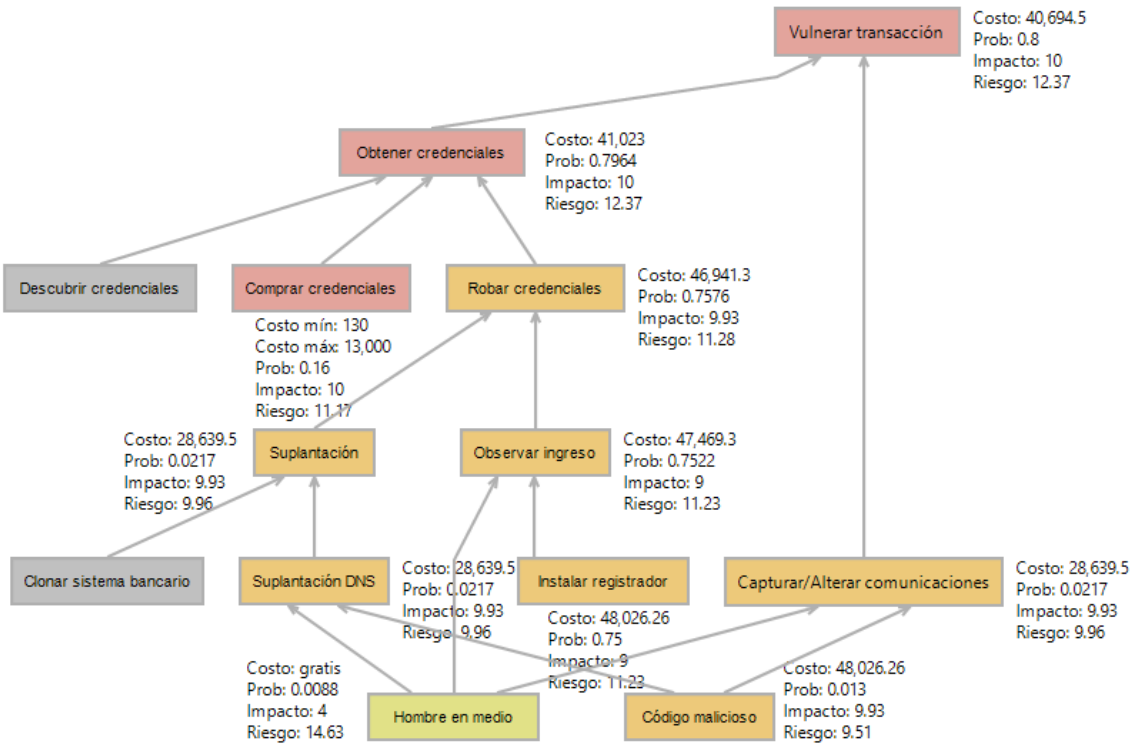


Figura 27. Nodos mitigados por controles (gris) en el árbol completo.

Estos números podrían ser aún más favorables, al grado de alcanzar una probabilidad de alrededor del 20%, si las herramientas adicionales diseñadas para proteger contra el registro de teclas no presentaran vulnerabilidades suficientemente serias como para inutilizar este tipo de funciones (Figura 28.)

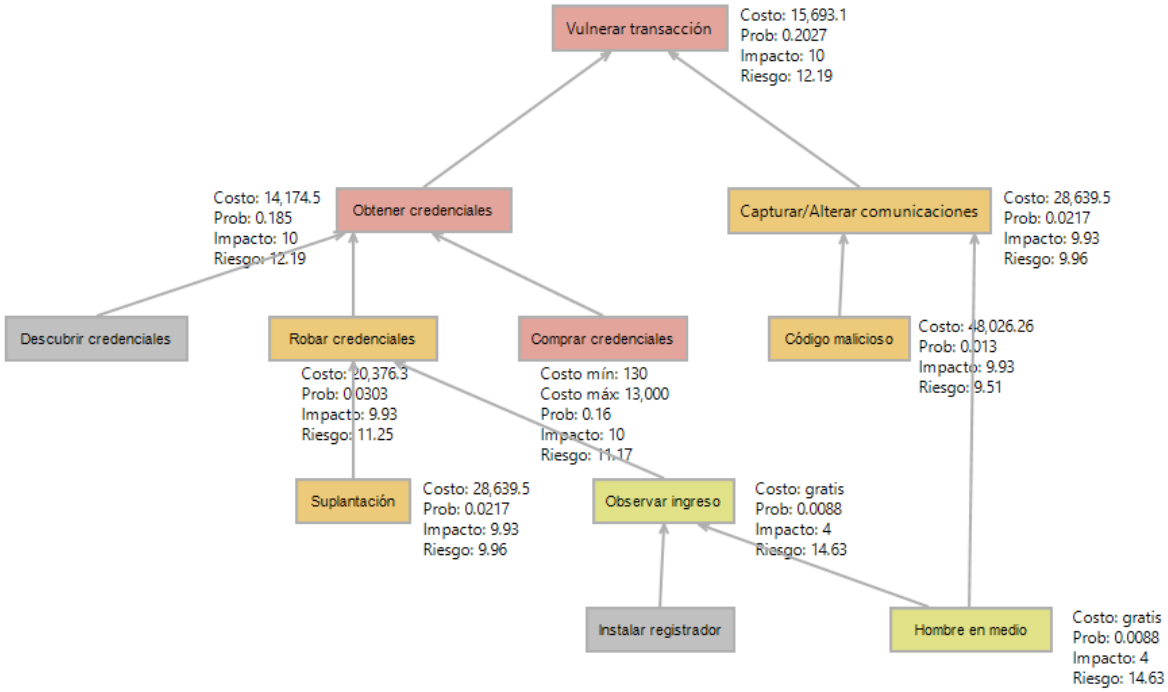


Figura 28. Nodos mitigados por controles (gris) en el árbol completo.

Es evidente entonces lo relevante y útil que resulta el preocuparse por la educación de los usuarios de los sistemas de banca electrónica, no sólo como complemento a los controles técnicos, sino como un objetivo principal en los planes de seguridad de las instituciones financieras. Si bien se afirma que en el caso mexicano la incidencia de fraudes electrónicos ha disminuido y su impacto monetario es menor, encontrar la motivación suficiente para continuar invirtiendo en la seguridad de los sistemas será complicado mientras se mantenga la idea de que investigar el origen de los fraudes es menos redituable que costearlos [56].

A continuación se describe con un mayor detalle la subcategoría de banca móvil, tras lo cual se efectuará un análisis similar al presentado en este capítulo, en el contexto de los dispositivos móviles, con la finalidad de realizar una comparativa de las problemáticas asociadas a las diferentes plataformas.

# 5. Banca móvil

En los últimos tiempos, la venta de computadoras personales a nivel mundial ha decaído de manera constante a favor de los dispositivos móviles. En 2013, la adquisición de equipos de cómputo se redujo un 10.6% [57] (de 340 a 305 millones de unidades) en comparación con 2012, mientras que la de las tabletas y teléfonos inteligentes aumentaron 67.9% (de 120 a 200 millones) y 46.5% [58] (de 154 a 225 millones, comparando los segundos cuartos del 2012 y 2013) respectivamente.

La gran penetración de estas nuevas plataformas, al grado de considerarlas una extensión de nuestro cuerpo, ha provocado que varias compañías e instituciones migren sus servicios a éstas o que incluso ofrezcan nuevos, con la finalidad de no perder presencia en el mercado al seguir con las preferencias internacionales. Los servicios financieros no han sido la excepción, por lo que a pesar del uso generalizado que la banca a través de internet ha alcanzado, la banca móvil ha ganado terreno de manera significativa.

La banca móvil se trata del ofrecimiento de servicios bancarios a través de dispositivos móviles, cuya línea telefónica asociada debe encontrarse ligada a las transacciones que se realicen[61]. Los servicios a los que se puede acceder por estos medios son similares a aquellos que la banca por internet ofrece [59].

En Estados Unidos, el número de usuarios de la banca móvil ha aumentado 7.5 millones en 9 meses, mientras que en Europa se sigue el mismo camino: entre agosto del 2010 y marzo del 2011, los usuarios de la banca móvil aumentaron 40% entre los propietarios de teléfonos inteligentes en Reino Unido, Francia, España, Alemania e Italia [60]. En nuestro país, sin embargo, estas tendencias aún no se ha establecido: de acuerdo al Instituto Nacional de Estadística y Geografía y la Comisión Nacional Bancaria y de Valores [61], en el 2012 sólo el 2% de los mexicanos bancarizados utilizó la banca a través de dispositivos móviles de manera regular (alrededor de 1.5 millones, lo cual es contrastante con los 32 millones en la Unión Americana.)

Las cifras anteriores, más que ser desalentadoras, evidencian el gran potencial de crecimiento que tiene nuestro país en esta materia. En 2012, la penetración de los teléfonos inteligentes en México fue de alrededor de 20% [62], pero se proyecta que para 2015 siete de cada diez teléfonos sean inteligentes [63], lo que motivará a que los bancos aprovechen la proliferación de estos dispositivos para atraer a más usuarios a los servicios financieros y a que la banca móvil comience a ser una necesidad y no una elección.

## 5.1 Tipos de banca móvil

Existen tres principales tipos de banca móvil, consistentes con las funcionalidades de los diferentes modelos de teléfonos existentes en el mercado: a través de mensajes SMS, a través de una conexión a internet inalámbrica/GSM o a través de aplicaciones dedicadas que las instituciones financieras distribuyen a sus cuentahabientes.

- Pago móvil. Este servicio se encuentra orientado a aquellos usuarios que, a pesar de no contar con un dispositivo inteligente, desean utilizar algunas de las funcionalidades de la banca móvil. Consiste básicamente en el intercambio de

[61] Si las transacciones realizadas en un dispositivo no se encuentran ligadas a una línea telefónica, entonces se considera que se está haciendo uso de la banca por internet, no de la banca móvil.

mensajes SMS con la institución bancaria para realizar tanto consultas como transacciones: el cliente envía un mensaje de texto con un formato específico al banco, quien lo procesa y responde a la solicitud a través del mismo medio.

Las respuestas toman la forma de notificaciones de los movimientos realizados por el cuentahabiente, ya sea de manera directa en alguna sucursal o por medios electrónicos, directamente a su teléfono.

Para realizar transacciones, el usuario debe conocer el código de cada una de ellas (generalmente alfanumérico) y solicitarla en un mensaje, por lo que si no se tiene una guía o familiaridad con los servicios existentes pueden suscitarse errores al procesarse transacciones no deseadas, lo que podría considerarse un inconveniente de esta clase de servicio.

- Internet móvil. De manera adicional al servicio de voz que un proveedor ofrece a sus clientes, un dispositivo móvil puede contar con el servicio de datos si éste se tiene contratado. A través de él un usuario puede acceder a los servicios financieros de su banco, ya sea mediante una aplicación específica para su teléfono o tras visitar el portal web o móvil de la institución financiera en un navegador, aunque esta última modalidad no se considera banca móvil.

## 5.2 Riesgos de la banca móvil

La mayoría de los riesgos no discutidos en la sección de banca electrónica están directamente relacionados con los dispositivos móviles introducidos en el análisis, así como con las aplicaciones que se ejecutan en ellos.

Este tipo de equipos se encuentran expuestos a los mismos riesgos que una computadora conectada a internet, además de los riesgos propios del uso de una red inalámbrica, del uso de los servicios de banca electrónica y aquellos que han aparecido conforme su popularidad y penetración han aumentado.

En lo referente al riesgo operacional, existen igualmente tres puntos susceptibles a ser vulnerados durante una transacción: usuarios, canales de comunicación y aplicaciones bancarias.

### 5.2.1 Usuarios

Muchos usuarios tienen cierta conciencia respecto a las vulnerabilidades de sus computadoras, pero la mayoría de las veces consideran que sus dispositivos móviles son tan seguros como su línea telefónica tradicional, por lo que no tienen inconveniente alguno en proveer a sus equipos con una gran cantidad de información personal (contactos, redes sociales, ubicación, etc.) y financiera. Lo anterior, en conjunto con la falta de criterio respecto a la descarga e instalación de aplicaciones y la práctica tan común de "liberar" o "rootear" los dispositivos[62], explica la gran cantidad de código malicioso dedicado que existe. Entre 2011 y 2012, el código malicioso para dispositivos móviles aumentó un 163% [64], acercándose a las 65 mil piezas de software dañinas.

[62] Al remover las limitaciones de dispositivos con sistemas operativos iOS o Android se alcanzan permisos de administrador en los mismos, lo cual puede facilitar la labor de aplicaciones maliciosas instaladas debido a que éstas heredan el acceso total asociado a tales privilegios.

En este sentido, los atacantes suelen aprovechar medios inseguros de distribución, como Google Play o Cydia, para hacer llegar a los usuarios aplicaciones maliciosas que, entre otras cosas, pueden actuar de hombre en medio al imitar a las ofrecidas de manera legítima por las instituciones financieras, sin embargo, este medio de distribución no es el único existente. En los últimos meses se ha demostrado que actividades universalmente consideradas inofensivas, como recargar la batería de un dispositivo, puede derivar en inyección de código malicioso [65].

Además de las aplicaciones fraudulentas, las redes de bots tan presentes en las computadoras personales han comenzado a adaptarse para expandir su campo de acción al nuevo paradigma móvil, por ejemplo, las nuevas versiones de los bot ZeuS y SpyEye contienen módulos destinados a robar segundos factores de autenticación en los canales considerados "fuera de banda", como mensajes de texto cortos o generadores emulados en teléfonos inteligentes [66]. Un ejemplo de lo anterior puede observarse en las modificaciones de los ataques clásicos de suplantación, en los que en la actualidad es solicitada adicionalmente información referente a dispositivos móviles, como números telefónicos, que son utilizados para hacer llegar ligas maliciosas dentro de mensajes de texto corto a los equipos.

Una de las razones que permiten este tipo de ataque en las nuevas plataformas, además del siempre presente factor social, es el tamaño de los dispositivos. Al no contar con las pantallas propias de las computadoras personales, se torna un tanto más complicado el verificar la seguridad de la conexión y del sitio que se visita. En algunos, la visualización de las direcciones web desaparece una vez que la página ha sido descargada, por lo que en primera instancia complica la comprobación del uso de protocolos como SSL.

Otro punto a tratar es el referente a los sistemas operativos con los que todo dispositivo móvil cuenta. Cada uno de ellos presenta en algún momento vulnerabilidades que, de ser explotadas, pueden comprometer con diferente grado de criticidad las funcionalidades de los sistemas, por ejemplo, permitir el acceso parcial [67] o total [68] a los dispositivos debido a fallas en los sistemas de bloqueo y autenticación, o permitir la modificación de aplicaciones legítimas firmadas digitalmente para añadir funcionalidades propias de los caballos de Troya [69].

Dejando a un lado lo referente a vulnerabilidades y código malicioso, este tipo de equipos se encuentran igualmente expuestos a ataques menos elaborados pero no por ello menos relevantes. De manera similar al caso de los servicios bancarios a través de computadoras personales, los usuarios de dispositivos móviles son susceptibles a la utilización de redes inseguras, con la diferencia de que en este caso existen dos posibles puntos de riesgo de acuerdo al tipo de conexión que se establezca: las redes GSM y las redes inalámbricas, ambas vulnerables a ataques de hombre en medio.

Finalmente, el robo o extravío de dispositivos combinado con el uso de contraseñas de desbloqueo débiles o la total ausencia de ellas, pone igualmente a disposición de un atacante una gran cantidad de información sensible.

### 5.2.2 Canales de comunicación

Como se mencionó anteriormente, en este sentido pueden identificarse algunas variaciones en los medios de comunicación dependiendo del tipo de acceso a los servicios financieros. Cuando un usuario utiliza una red inalámbrica se establece un canal de comunicación entre éste y las instituciones bancarias mediante un proveedor de

servicios de internet, mientras que al utilizar un plan de datos se presenta un canal adicional, el de la red entre el dispositivo y el proveedor de servicios móviles, previo a la comunicación por internet con los bancos.

Al igual que las redes inalámbricas, las redes móviles son susceptibles a los ataques de hombre en medio, por ejemplo, a través de la suplantación de una torre de transmisión. Dado que los dispositivos móviles se conectan a la torre con la señal más potente en el área al momento, un atacante podría interceptar todo tipo de información simplemente al lograr emitir una señal con la intensidad suficiente e indicar a los equipos capturados que descarten la utilización de cualquier cifrado [70].

A pesar de que las redes móviles presentan varias vulnerabilidades con pruebas de concepto existentes [71], como el caso anterior, los conocimientos técnicos y el equipo necesario para comprometer este canal de comunicación son mucho más complejos en comparación con el caso de las redes inalámbricas, por lo que si bien no son garantía de seguridad, sí es menos probable un intento de ataque a este tipo de conexión [72].

### 5.2.3 Aplicaciones bancarias

Como se mencionó anteriormente, la utilización de los servicios financieros móviles puede realizarse mediante aplicaciones dedicadas o a través del navegador web de los dispositivos.

En muchas ocasiones, debido a malas prácticas y malos diseños, la mayoría de las aplicaciones móviles hacen un pobre manejo de los datos personales de los usuarios. De 50 aplicaciones muy populares para iPhone y Android, sólo 3 hacen un correcto uso y administración de la información sensible [73], por lo que el peligro no sólo reside en el uso de aplicaciones con código malicioso oculto, sino igualmente en el uso de las legítimas.

Varios de los problemas en el manejo de datos tienen que ver con deficiencias en el cifrado de información residente en los dispositivos, por ejemplo, credenciales de acceso, información personal y financiera almacenada en claro, etcétera. De igual manera, en algunas ocasiones no se realiza una correcta validación de certificados digitales por parte de las aplicaciones con esta funcionalidad, por tanto, el establecimiento de los canales de comunicación seguros y la confidencialidad/integridad de la información que viaja por ellos es al menos cuestionable.

En el caso de la infraestructura bancaria, los servidores dedicados a ofrecer estos servicios se encuentran expuestos los mismos riesgos que sus contrapartes de banca por internet enfrentan, por ejemplo, la denegación de servicio.

## 5.3 Medidas de seguridad

De manera consecuente a lo señalado para la banca electrónica, en la que los servicios móviles se encuentran incrustados, las medidas de seguridad de la banca móvil también consideran la perspectiva tecnológica y la regulatoria.

### 5.3.1 Controles tecnológicos

En este sentido, salta a la vista un punto de control, adicional al canal de comunicación y al propio usuario, propio de la plataforma en que las transacciones se realizan bajo esta modalidad: las aplicaciones bancarias para dispositivos móviles.

#### *5.3.1.1 Usuario*

El primer punto de control es la autenticación del usuario en el dispositivo utilizado para realizar transacciones financieras. Las ofertas de dispositivos que existen en la actualidad implementan diferentes mecanismos de desbloqueo, que pueden consistir en códigos numéricos de al menos cuatro dígitos, bloqueo por patrón o la captura de ciertas características biométricas.

Esta autenticación de un solo factor no es suficiente para algunos servicios de la banca móvil, por lo que de manera similar al caso de banca electrónica, un doble factor fuera de banda es utilizado para transacciones de mayor cuantía (identificador es el número de teléfono, no se requiere para pago móvil), con la diferencia de que el canal de comunicación sobre el cual el factor adicional es transmitido debe ser diferente al dispositivo móvil en el que las transacciones financieras serán ejecutadas (tarjeta SIM se considera un factor.)

Considerando ahora código malicioso, diversas compañías han comenzado a desarrollar sistemas de detección/prevención de intrusos para dispositivos móviles [74] que, en conjunto con la cada vez mayor oferta de soluciones antivirus especializadas, buscan mitigar las amenazas de hombre en medio y suplantación. Por otro lado, las aplicaciones financieras bien diseñadas se ejecutan en un ambiente aislado (cajas de arena) en el que los recursos son limitados y predeterminados, de tal manera que si una brecha se suscita, el acceso a recursos fuera de ese entorno por parte de una entidad maliciosa es muchísimo más complicado.

Una medida de protección adicional para el caso de suplantación son las liberaciones recientes de navegadores web "seguros" [75], que trasladan a los paradigmas móviles varios de los mecanismos discutidos en capítulos anteriores. La idea principal es tratar de reducir al mínimo la toma de decisiones de seguridad a los usuarios mediante la revisión exhaustiva de cada dirección ingresada contra una lista negra almacenada en una nube, con el consecuente bloqueo del acceso al sitio si éste es encontrado en el listado. Además de lo anterior, es posible el bloqueo predeterminado de sitios con base en tipos de contenido (pornografía, drogas, violencia, redes sociales, etc.)

Finalmente para el caso de robo o extravío, además del control de acceso básico mencionado anteriormente, algunos proveedores de servicios móviles han comenzado a ofrecer la posibilidad de bloquear los dispositivos a través del código IMEI, que en conjunto con la funcionalidad de borrado remoto incluida en varios equipos, permite mantener un cierto grado de confidencialidad en la información personal almacenada.

#### *5.3.1.2 Canal de comunicación*

Los controles implementados para la protección de redes móviles generalmente se enfocan en la intercepción y suplantación de las comunicaciones, así como el evitar que un usuario pueda ser rastreado a través de su dispositivo [76].

Con el objetivo anterior, las comunicaciones a través de este canal de comunicación viajan cifradas mediante el algoritmo A5 o A3 que, si bien no es perfecto debido a la longitud de su llave (64 bits), protege contra ataques simples de intercepción de llamadas o mensajes.

Otra buena práctica consiste en una autenticación estricta, en la que los dispositivos involucrados deben generar una nueva llave de cifrado por cada llamada o mensaje. Esta generación requiere aproximadamente medio segundo para suscitarse, por lo que desafortunadamente los proveedores de servicio no suelen implementarlo, debido a que asignan una mayor prioridad a disminuir el tiempo en que los datos se encuentran listos para salir.

Para reducir la posibilidad de rastreo, se utiliza el encaminamiento casero (home routing), que básicamente consiste en que todos los datos generados hacia un destinatario específico, sin importar que la conexión se realice entre proveedores diferentes, pasen antes por una plataforma "casera" intermedia que hace entrega de los datos a su cliente, desde la propia red a la que éste se encuentra afiliado [77] (Figura 29), de tal manera que la información relacionada con ubicación permanece inaccesible desde fuentes públicas.

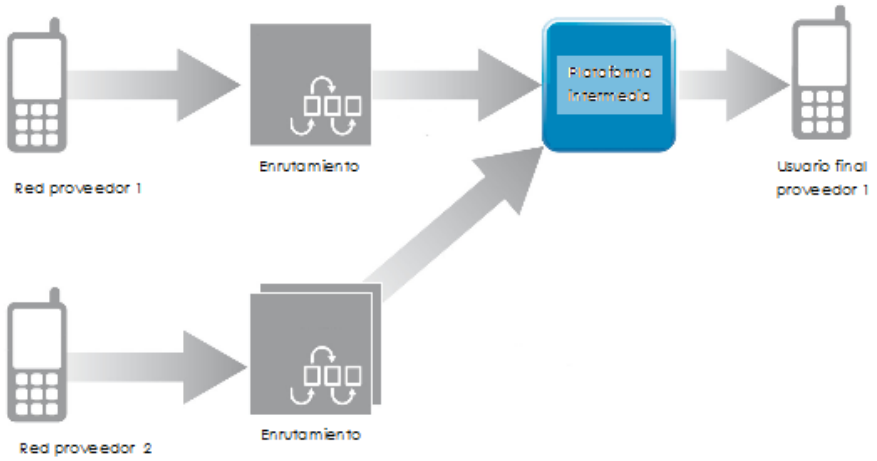


Figura 29. Encaminamiento casero[63].

### *5.3.1.3 Aplicaciones bancarias*

Una mejora en la seguridad de las aplicaciones utilizadas en la banca móvil parte de un buen diseño desde el origen. Algunas organizaciones como OWASP [78], han comenzado a desarrollar estándares y buenas prácticas de desarrollo para dispositivos móviles, los cuales consideran puntos como los siguientes:

- Identificación y protección de datos sensibles en los dispositivos.
- Manejo seguro de credenciales de autenticación.
- Protección de datos sensibles en tránsito.
- Correcta implementación de la autenticación, autorización y administración de las sesiones.
- Integración segura con servicios y aplicaciones de terceros.

[63] Basada en "The Case for SMS Home Routing", de Telsis.

- Control del acceso a los recursos de los dispositivos, como mensajes de texto y llamadas telefónicas.

- Aseguramiento de los medios para la distribución de actualizaciones y parches de seguridad.

- Correcto manejo de errores en tiempo real.

De manera adicional al seguimiento de estándares de codificación, es igualmente recomendable ejecutar revisiones de código, ya sea de manera interna o por auditores externos a las instituciones. Algunas maneras de atender este punto son los análisis estáticos y dinámicos, los cuales se cree que en conjunto pueden llegar a identificar hasta el 95% de los errores en una aplicación [79].

En un análisis estático se realiza únicamente la revisión del código, buscando identificar el uso de librerías vulnerables y la correcta codificación de los controles de seguridad diseñados. Por otro lado, en el análisis dinámico se estudia el comportamiento de la aplicación en ejecución, verificando la interacción de la misma con otros componentes como bases de datos, servidores, etc. Además de lo anterior, se fuerza el ingreso de datos específicos para probar el manejo de errores en ciertas zonas del código.

Finalmente, otra alternativa para la auditoria de aplicaciones consiste en la puesta en marcha de pruebas de penetración.

### 5.3.2 Controles regulatorios

Como ya se mencionó, los principales estándares en el contexto de la banca móvil están relacionados con la codificación segura, sin embargo, debido a que esta manera de realizar transacciones financieras forma parte de la banca electrónica tradicional, se encuentra regida igualmente por los mismos estándares y regulaciones que ésta.

Retomando el décimo capítulo de la Circular Única de Bancos, resulta importante mencionar algunas reglamentaciones adicionales a las ya señaladas en capítulos anteriores, diseñadas para la utilización de la banca electrónica a través de dispositivos móviles:

- Una cuenta de usuario debe estar forzosamente ligada a un solo número de línea telefónica y, de igual manera, un número de línea telefónica no puede estar ligado a dos dispositivos móviles.

- Cada línea telefónica puede tener asociados hasta dos números de tarjeta o de cuenta, siempre y cuando uno de ellos sea utilizado exclusivamente para micropagos[64].

- El identificador de usuario en una transacción de pago o banca móvil toma la forma del número de línea telefónica, obteniendo éste directamente del dispositivo.

- En lo referente a factores de autenticación de categoría 2, la única restricción es que la longitud utilizada sea de cinco caracteres, siempre y cuando las

[64] El equivalente en moneda nacional al rango comprendido entre cero y 25 dólares estadounidenses.

instituciones financieras hagan constante énfasis en la importancia de una contraseña robusta. Por otro lado, cualquier mecanismo utilizado para verificar que el dispositivo o la línea telefónica se encuentran autorizados para la realización de transacciones, puede ser considerado un factor de clase 3.

- El uso pago móvil no requiere un factor de autenticación adicional al número de línea telefónica ni el registro de cuentas destino si las transacciones realizadas caen en el orden de micropagos.

- El uso pago móvil no requiere el registro de cuentas destino, pero sí precisa un NIP, si las transacciones realizadas caen en el orden de baja cuantía[65].

- El uso pago móvil requiere el registro de cuentas destino y de un NIP, si las transacciones realizadas caen en el orden de mediana cuantía[66].

- El uso de la banca móvil requiere el registro de cuentas destino, el uso de dos factores de autenticación, el cifrado de información y de la notificación de movimientos a los usuarios. Adicionalmente, los límites transaccionales comprenden desde los 530 dólares hasta el monto establecido por cada institución financiera [59].

- Los usuarios pueden establecer límites de monto adicionales para las operaciones monetarias, sin exceder las cantidades de mediana cuantía o los 4000 dólares mensuales. Es prerrogativa de las instituciones financieras el establecer límites inferiores a los mencionados.

- La notificación a los usuarios con respecto a los movimientos realizados debe ser inmediata cuando el monto acumulado diario sea mayor a 600 dólares o cuando una transacción individual exceda los 250 dólares.

Finalmente, es importante hacer énfasis nuevamente en que dentro de las regulaciones establecidas se considera la obligación que tienen las instituciones de comunicar los riesgos inherentes al uso de los servicios electrónicos y de los dispositivos a través de los cuales se acceden, así como la difusión de sugerencias para mitigar riesgos y así reducir la incidencia de operaciones irregulares o ilegales.

La adopción de las plataformas móviles introduce una nueva serie de temáticas propias de los equipos y medios de transmisión adicionales, así como la modificación de algunas situaciones de riesgo previamente identificadas a plenitud, las cuales deben ser incluidas dentro de los esfuerzos de concientización complementarios a los controles tecnológicos.

[65] El equivalente en moneda nacional al rango comprendido entre 25 y 90 dólares estadounidenses.
[66] El equivalente en moneda nacional al rango comprendido entre 90 y 530 dólares estadounidenses.

# 6. Análisis del riesgo en el uso de la banca móvil mediante árboles de ataque

Como ya se mencionó en capítulos anteriores, los análisis realizados correspondientes a la banca electrónica a través de computadoras personales tienen la finalidad de establecer antecedentes en su uso y riesgos asociados al mismo, buscando establecer una comparativa con los resultados emanados del ejercicio desarrollado en el presente capítulo, referentes a la banca móvil, identificando así cuáles problemáticas siguen presentes, cuáles se introducen a la par de los nuevos dispositivos y, en su caso, las maneras en que se pretende atenderlas.

En este capítulo no se realizan análisis adicionales referentes a la infraestructura bancaria, ya que lo descrito anteriormente es aplicable a los nuevos servicios que se incluyen a continuación.

## 6.1 Identificación de activos

### 6.1.1 Usuarios

De manera similar al caso analizado previamente, el activo indispensable para acceder a los servicios es un dispositivo móvil.

Si una aplicación bancaria dedicada es utilizada, ésta servirá como interfaz entre el usuario y el sistema de autenticación correspondiente, ya sea mediante la solicitud de identificadores de usuario y una o más contraseñas en cada sesión o mediante la provisión de información almacenada dentro del propio dispositivo, por lo que estas credenciales de acceso son igualmente un activo al cual se debe prestar atención.

Un activo adicional a tomar en cuenta, aplicable únicamente a este tipo de servicios, es la información referente al número de línea telefónica asociada al dispositivo, ya que a través de ella pueden iniciarse vectores de ataque como el de suplantación de identidad.

### 6.1.2 Canales de comunicación

En el caso de este tipo de servicios, el activo es igualmente el canal por sí mismo, con la diferencia de que existirán dos medios diferentes (Wi-Fi o red móvil) de acuerdo al tipo de conexión utilizada.

## 6.2 Identificación de amenazas

### 6.2.1 Hacia el usuario

La amenaza hacia las credenciales de usuario y en general hacia cualquier tipo de información personal, consiste en que ésta pierda su confidencialidad de alguna manera. Tal pérdida, si bien puede derivarse de un ataque lógico contra los sistemas y servicios, igualmente puede estar ligada a la pérdida física de los dispositivos, lo cual constituye otra amenaza.

Finalmente, las instituciones establecen que sus cuentahabientes deben atender a un cierto número mínimo de recomendaciones de seguridad para la realización de transacciones en su dispositivo, por tanto, la amenaza consiste en la pérdida de ese estado óptimo.

**Árbol de ataque**

Objetivo: **Obtener credenciales de usuario** (Figura 30.) Costo: 329.79 pesos, probabilidad: 0.8849, impacto: 10, riesgo: 4.76.

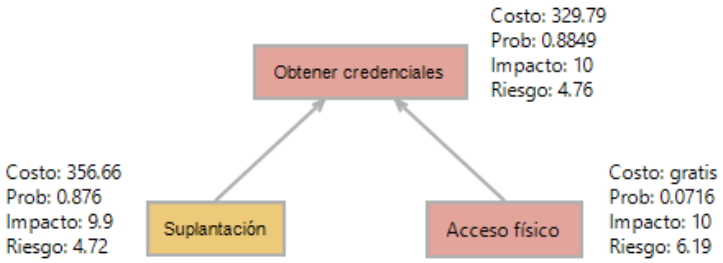


Figura 30. Árbol de ataque simplificado, cuyo objetivo es la obtención de credenciales de usuario.

1. **Suplantación** (OR, Figura 31.) Costo: 356.66 pesos, probabilidad: 0.876, impacto: 9.9, riesgo: 4.72.

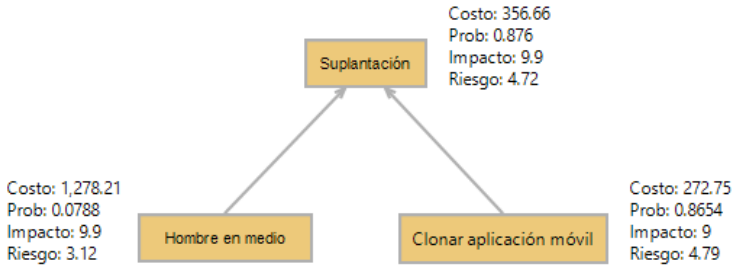


Figura 31. Especificación de la rama "Suplantación."

La suplantación de aplicaciones móviles, uno de los medios de distribución de código malicioso más recurrentes en la actualidad, no es un vector de ataque con demasiada dificultad. Si bien las compañías líderes en este mercado establecen medidas estrictas para evitar que se ofrezcan aplicaciones fraudulentas en sus plataformas, lo cierto es que muchas de ellas logran estar en línea aún cuando sea por un breve periodo de tiempo. Por otro lado, la existencia de tiendas alternativas para dispositivos "liberados" facilita igualmente la distribución inadvertida.

El único requerimiento para comenzar a desarrollar este tipo de aplicaciones consiste en una licencia anual por parte del proveedor, la cual puede obtenerse de manera gratuita para instituciones educativas y a un precio de 99 dólares para individuales [80].

En el año 2012 el número de aplicaciones existentes para Android alcanzó las 700,000 [81], la mitad de las cuales fueron identificadas como maliciosas o de alto riesgo y 52.16% de ellas tenían la funcionalidad de robar información personal, de descargar código malicioso adicional o de obtener permisos de administrador en el dispositivo [82].

$$Prob: = \frac{Aplicaciones\ con\ características\ maliciosas\ específicas}{Número\ de\ aplicaciones\ existentes} = \frac{182{,}560}{700{,}000} = 0.2608$$

Otro medio de distribución, que puede estar asociado a la suplantación de identidad tradicional a través de computadoras personales, es mediante ligas en mensajes de texto corto.

Si se le considera parte de un intento por obtener segundos factores de autenticación fuera de banda, se le puede asignar el mismo costo que el establecido para la clonación de sitios web bancarios observado en el capítulo cuatro, con la diferencia de que este ataque se volvería más amortizable, contando ahora con la posibilidad de agregar vectores de ataque adicionales por el mismo precio. Sin embargo, existen programas en el mercado que permiten el envío de múltiples mensajes de texto a diferentes destinatarios que, a pesar de estar destinados a campañas publicitarias, pueden ser utilizados como generados de correo no deseado por un costo inicial de 33 dólares [83].

En la actualidad, se cree que el nivel de correo no deseado en Norteamérica es de alrededor del 0.1% de todos los mensajes que circulan [84], 90% de los cuales son leídos en los primeros quince minutos después de ser recibidos y, si se considera una acción similar como lo es dar clic en una dirección provista mediante correo no deseado, se tiene una probabilidad de 0.1 de seguir la liga de un SMS. Sin embargo, se cree igualmente que los usuarios de dispositivos móviles son tres veces más propensos a ser víctimas de una suplantación de identidad [85] en comparación con usuarios de computadoras personales, por lo que la probabilidad antes mencionada crecería a 0.3.

1.1 **Clonar aplicación móvil** (OR, Figura 32.) Costo: 1,278.21 pesos, probabilidad: 0.0788, impacto: 9.9, riesgo: 3.12.

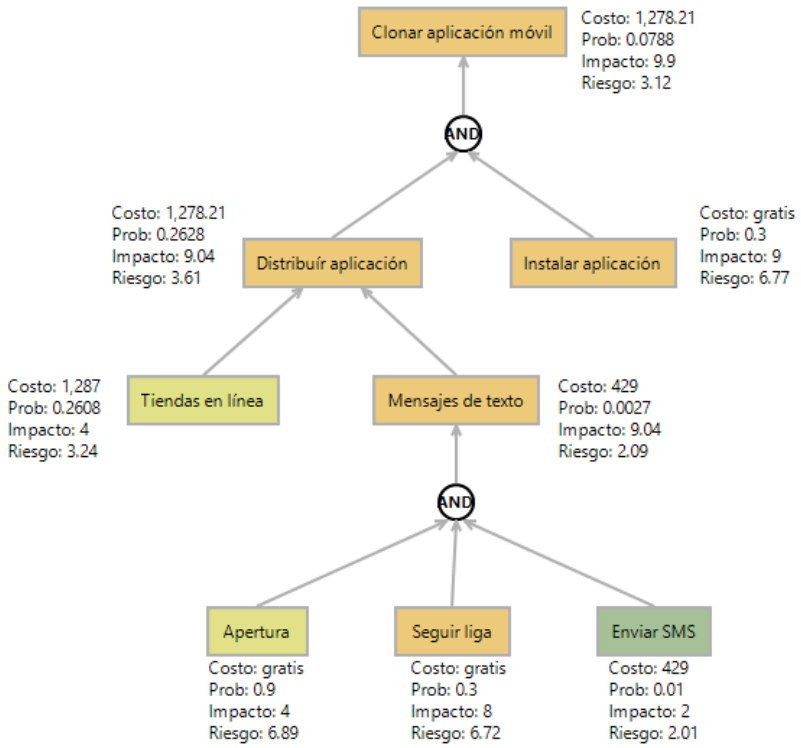


Figura 32. Especificación de la rama "Clonar aplicación móvil."

1.1.1 **Distribuir aplicación** (AND.) Costo: 1,278.21 pesos, probabilidad: 0.2628, impacto: 9.04, riesgo: 3.61.

1.1.1.1 **Distribuir a través de tiendas en línea** (OR.) Costo: 1,287 pesos, probabilidad: 0.2608, impacto: 4, riesgo: 3.24.

1.1.1.2 **Distribuir mediante ligas en mensajes de texto cortos** (OR.) Costo: 429 pesos, probabilidad: 0.0027, impacto: 9.04, riesgo: 2.09.

1.1.1.2.1 **Enviar mensaje de texto corto** (AND.) Costo: 429 pesos, probabilidad: 0.01, impacto: 2, riesgo: 2.01.

1.1.1.2.2 **Abrir mensaje de texto corto** (AND.) Costo: gratuito, probabilidad: 0.9, impacto: 4, riesgo: 6.89.

1.1.1.2.3 **Seguir liga de mensaje de texto corto** (AND.) Costo: gratuito, probabilidad: 0.3, impacto: 8, riesgo: 6.72.

1.1.2 **Instalar aplicación** (AND.) Costo: gratuito, probabilidad: 0.3, impacto: 9, riesgo: 6.77.

1.2 **Realizar ataque de hombre en medio** (OR, Figura 33.) Costo: 272.75 pesos, probabilidad: 0.8654, impacto: 9, riesgo: 4.79.

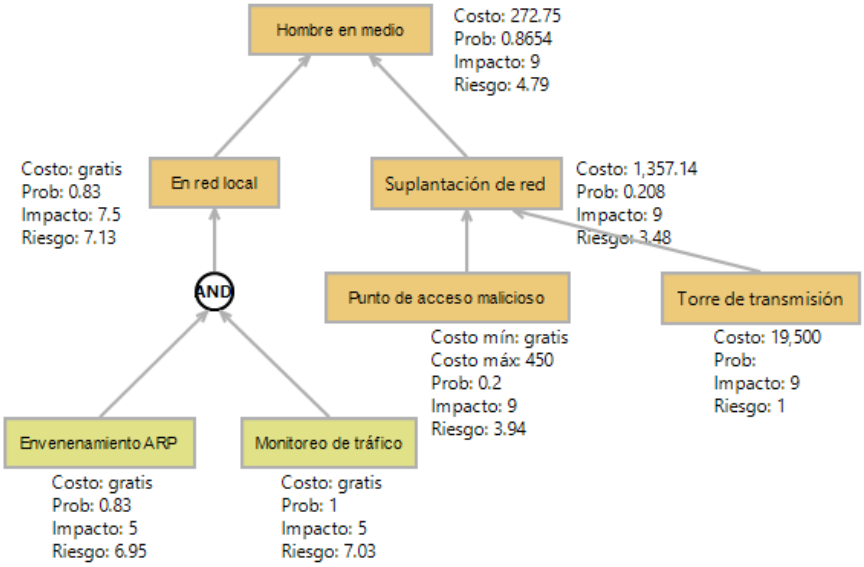


Figura 33. Especificación de la rama "Hombre en medio."

Las métricas correspondientes a los ataques de hombre en medio en una red local y a través del establecimiento de un punto de acceso Wi-Fi se mantienen, debido a que éstos no se modifican con la introducción de nuevos dispositivos. La nueva variante, suplantación de una antena de transmisión móvil, puede ser lograda mediante dispositivos con costo de al menos 1,500 dólares [70]. Si bien es complicado determinar un valor probabilístico debido a que no se tiene el dato exacto referente al número de antenas fraudulentas (tanto por parte de atacantes como de agencias de espionaje gubernamental) existentes, es muchísimo más probable encontrarse con un punto de acceso malicioso.

1.2.1 **Realizar ataque de hombre en medio en red local inalámbrica** (OR.) Costo: gratuito, probabilidad: 0.83, impacto: 7.5, riesgo: 7.13.

1.2.1.1 **Envenenar protocolo ARP** (AND.) Costo: gratuito, probabilidad: 0.83, impacto: 5, riesgo: 6.95.

1.2.1.2 **Monitorear tráfico de red** (AND.) Costo: gratuito, probabilidad: 1, impacto: 5, riesgo: 7.03.

1.2.2 **Suplantar red inalámbrica o móvil** (OR.) Costo: 1,357.14 pesos, probabilidad: 0.208, impacto: 9, riesgo: 3.48.

1.2.2.1 **Crear punto de acceso Wi-Fi malicioso** (OR.) Costo: 450 pesos, probabilidad: 0.2, impacto: 9, riesgo: 3.94.

1.2.2.2 **Crear torre de transmisión móvil maliciosa** (OR.) Costo: 19,500 pesos, impacto: 9, riesgo: 1.

2. **Acceder físicamente a dispositivo** (OR, Figura 34.) Costo: gratuito, probabilidad: 0.0716, impacto: 10, riesgo: 6.19.

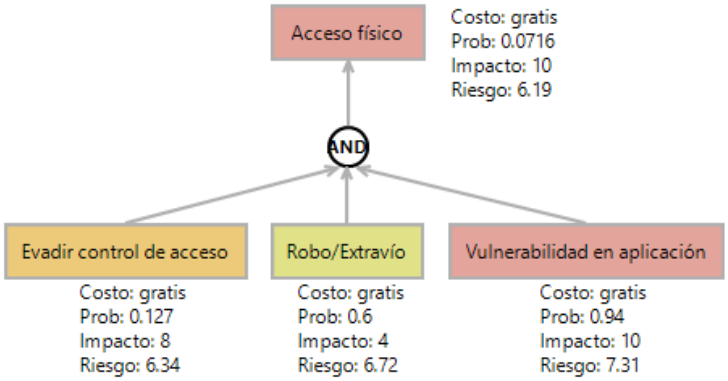


Figura 34. Especificación de la rama "Acceso físico."

De acuerdo a la compañía Lookout Mobile Security, desarrolladora de una aplicación que permite rastrear dispositivos móviles extraviados, en el año 2011 quince millones de equipos eran localizables por sus sistemas, de los cuales nueve millones de ellos fueron reportados como extraviados [86].

$$Prob: = \frac{Dispositivos\ robados/extraviados}{Dispositivos\ localizables} = \frac{9\ millones}{15\ millones} = 0.6$$

De llegar a las manos de un atacante por cualquier medio, éste puede intentar evadir el sistema de control de acceso al dispositivo. De las trescientas siete vulnerabilidades documentadas por el sitio CVE Details para el sistema operativo iOS, treinta y nueve de ellas están relacionadas con la evasión de la autenticación inicial [87].

$$Prob: = \frac{Vulnerabilidades\ de\ control\ de\ acceso}{Vulnerabilidades\ documentadas} = \frac{39}{307} = 0.127$$

Si finalmente es evadido el control de acceso al dispositivo, alguna vulnerabilidad de las aplicaciones podría intentar ser explotada. De cada cincuenta aplicaciones auditadas, sólo tres de ellas en promedio hace un correcto manejo de datos sensibles, tanto almacenados en el propio equipo como en tránsito [73].

$$Prob: = \frac{Aplicaciones\ vulnerables}{Aplicaciones\ auditadas} = \frac{47}{50} = 0.94$$

2.1 **Robar dispositivo/Encontrar dispositivo extraviado** (AND.) Costo: gratuito, probabilidad: 0.6, impacto: 4, riesgo: 6.72.
2.2 **Evadir control de acceso del dispositivo** (AND.) Costo: gratuito, probabilidad: 0.127, impacto: 8, riesgo: 6.34.
2.3 **Explotar vulnerabilidad de aplicaciones** (AND.) Costo: gratuito, probabilidad: 0.94, impacto: 10, riesgo: 7.31.

Del análisis realizado, salta a la vista en primera instancia que los costos de realización de los vectores de ataque lucen notablemente menores a los observados en la banca a través de internet. Esto puede ser debido a que la explotación de las vulnerabilidades identificadas no requiere que se acuda a los mercados negros dedicados al comercio de los bienes financieros, sino que son consecuencia de las habilidades en programación e ingeniería social de los atacantes.

Por otro lado, los valores del riesgo son igualmente menores, sin embargo, hay que recordar con son una simple referencia calculada en base al riesgo menor y a una función logarítmica. Debido a que en el análisis anterior se incluía la posibilidad, que resultó despreciable, de obtener credenciales de usuario realizando ataques de fuerza bruta y diccionario, el valor de referencia establecido fue notablemente más pequeño que el de banca móvil.

En cuanto a los resultados, a pesar de que un posible acceso físico al dispositivo conlleva un mayor nivel de riesgo como consecuencia de vulnerabilidades en aplicaciones, la suplantación en forma de hombre en medio en redes locales inalámbricas es el vector con mayor probabilidad de ocurrencia.

Siendo así, este riesgo y su criticidad se hereda desde la banca electrónica en la que los servicios financieros móviles se encuentran incrustados, reafirmando entonces la gran relevancia que tiene la participación de los usuarios en lo referente a su propia seguridad.

### 6.2.2 Hacia el canal de comunicación

En lo referente al canal de comunicación, la principal amenaza consiste en que el medio de transmisión pierda su carácter de "seguro", lo cual se encuentra considerado implícitamente en el ataque de hombre en medio incluido en las amenazas del lado del usuario.

## 6.3 Evaluación

Aunque las disposiciones regulatorias referentes a la cantidad de cuentas asociadas a los dispositivos son atendidas, en términos de funcionalidad no se hace mayor diferenciación entre banca a través de internet y banca móvil en algunos casos, por lo que las cuentas de usuario para ambos servicios son las mismas. Sin embargo, cuando la división se encuentra claramente definida y el usuario no desea la totalidad de los servicios electrónicos, el procedimiento para afiliarse a la banca móvil puede consistir en el registro vía telefónica o vía el servicio de banca a través de internet, con un posterior envío de mensajes de texto corto con códigos de activación y URL de descarga de la aplicación o en el registro directo desde el dispositivo.

Para acceder a la misma, cuando no se cuentan con todos los servicios, es imperativa la utilización del dispositivo y línea telefónica que se registró, la cual será solicitada en conjunto con una contraseña de entre cinco y seis dígitos numéricos como información

de autenticación, de lo contrario, las credenciales de banca por internet (números de cliente, contraseñas alfanuméricas, generadores de contraseñas dinámicas, etc.) serán utilizadas.

Aunque en general los nuevos servicios se encuentran contenidos dentro de la misma infraestructura de seguridad que la banca por internet [88], se establecen varias medidas de protección adicionales, como el hecho de que las sesiones en la aplicación expiran a los cinco minutos de inactividad, que no se almacena de manera local ningún tipo de información referente a consultas y transacciones y, cuando ésta se encuentra en tránsito, lo hace cifrada. El servicio ofrece la posibilidad de alertar al usuario, vía mensajes de texto o de correo electrónico, cuando se realicen movimientos mayores o iguales a 1,000 pesos y, además, establece límites monetarios en los traspasos entre cuentas propias, a terceros y a otros bancos, siendo éstos de entre 3,250 y 7,400 pesos por transacción, entre 7,400 y 19,500 pesos diarios y entre 29,500 y 52,000 pesos mensuales.

En uno de los casos se ofrece una modalidad de pago móvil, asociado a una cuenta de banca móvil, que consiste en la generación de tarjetas de crédito virtuales firmadas digitalmente utilizando contraseñas dinámicas. Tales tarjetas, de un solo uso por un monto específico, tienen una validez de 180 segundos.

De las medidas de seguridad mencionadas, sólo las referentes a la autenticación y al manejo de información en los equipos tienen impacto en la mitigación de los riesgos del lado del usuario previamente identificados, que son las más numerosas en este tipo de servicios. El resto tienen la finalidad de limitar el impacto monetario derivado de posibles vulneraciones en algún punto de los sistemas, los cuales son controles directamente emanados de las disposiciones regulatorias establecidas por la CNBV.

### 6.3.1 Rama "Acceso físico"

El robo/extravío de dispositivos puede ser mitigado mediante las funcionalidades de borrado remoto presentes en varios equipos, mientras que lo referente a vulnerabilidades de sistema operativo debe ser afrontado actualizando el software correspondiente cuando esto sea posible o deshabilitando las funciones vulnerables. Sin embargo, todas estas soluciones están condicionadas a la información y discernimiento de los usuarios que, de ser la adecuada, les permitiría tomar las decisiones correctas en pos de la seguridad de su información.

Por otro lado, las vulnerabilidades en el manejo de datos sensibles por parte de aplicaciones comienzan a ser atendidas a través de estándares y buenas prácticas en el ciclo de desarrollo. A pesar de lo anterior, los creadores del software móvil en estudio aseguran que éste no almacena ningún tipo de información en los dispositivos, por lo que idealmente esta rama se encuentra considerada en su totalidad (Figura 35.)

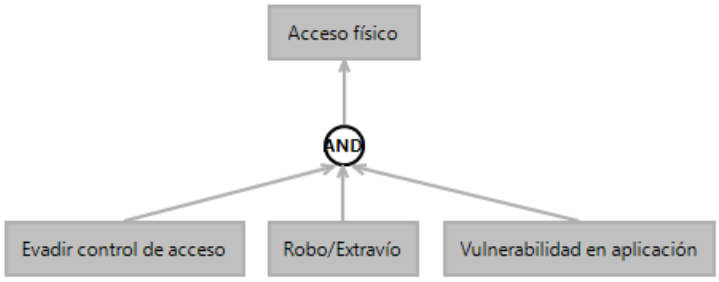


Figura 35. Nodos mitigados por controles (gris) en la rama "Acceso físico."

### 6.3.2 Rama "Suplantación"

En el caso de la suplantación de todo tipo, queda claro nuevamente que la participación del usuario es indispensable en la mitigación de los vectores de ataque. Sin embargo, sólo uno de los cinco casos estudiados ofrece recomendaciones de seguridad específicas para dispositivos móviles, limitándose el resto a la información correspondiente a banca por internet. Lo anterior, aunado al hecho de que en la actualidad no muchos usuarios han transferido la concientización y el buen criterio en lo referente a computadoras personales hacia el nuevo paradigma móvil, hace muy vulnerables a estos medios de transmisión hasta que nuevos esfuerzos sean llevados a cabo en este sentido.

Al igual que en el análisis de banca a través de internet, se considera a continuación el caso ideal en el que los usuarios pueden tomar decisiones de seguridad perfectamente informadas, con la finalidad de resaltar la gran importancia que los esfuerzos de información y difusión deben tener en los planes de seguridad de las instituciones.

La eventual aparición de piezas de software maliciosas en medios de distribución legítimos, como las tiendas en línea, o la recepción de mensajes de texto corto con direccionamientos fraudulentos es difícilmente erradicable, sin embargo, si los usuarios fueran capaces de diferenciar tales entidades de aquellas benignas, la instalación y consecuente robo de información sensible no se suscitaría, sin importar la proliferación de código malicioso para dispositivos móviles por múltiples canales (Figura 36.)

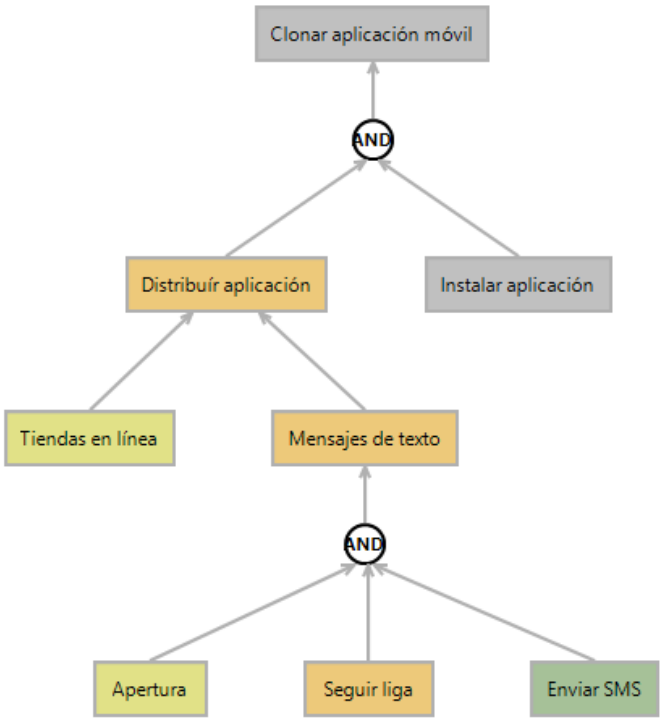


Figura 36. Nodos mitigados por controles (gris) en la rama "Clonar aplicación móvil."

Por otro lado, los usuarios serían más cuidadosos en lo referente a la red pública a la que se conectan y al tipo de transacciones que realizarían en ésta, aún cuando fuera legítima, por lo que el ataque de hombre en medio sería controlado casi en su totalidad (Figura 37.)

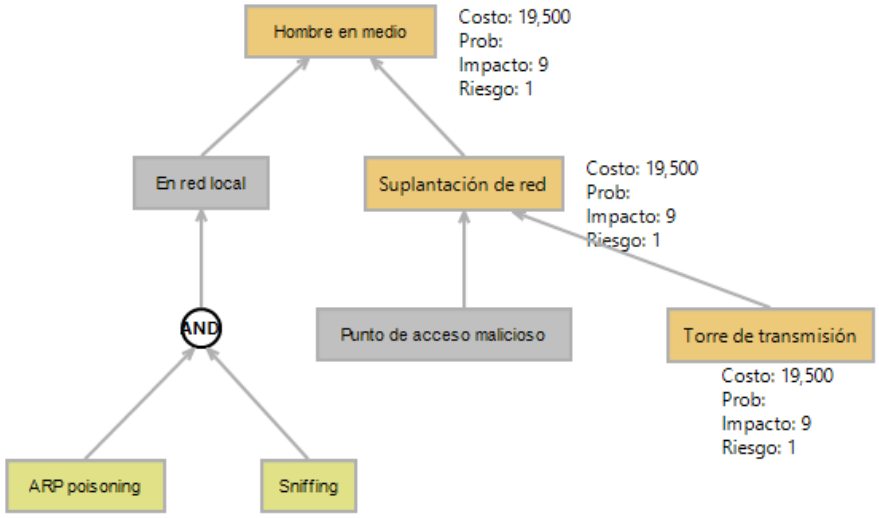


Figura 37. Nodos mitigados por controles (gris) en la rama "Hombre en medio."

Como puede observarse, la mitigación de los riesgos de la banca móvil considerando la participación de los usuarios es abismal, dado que el único vector de ataque restante sería la suplantación de antenas de transmisión que, como se mencionó anteriormente, es altamente improbable y costoso fuera de un contexto de vigilancia gubernamental (Figura 38.)

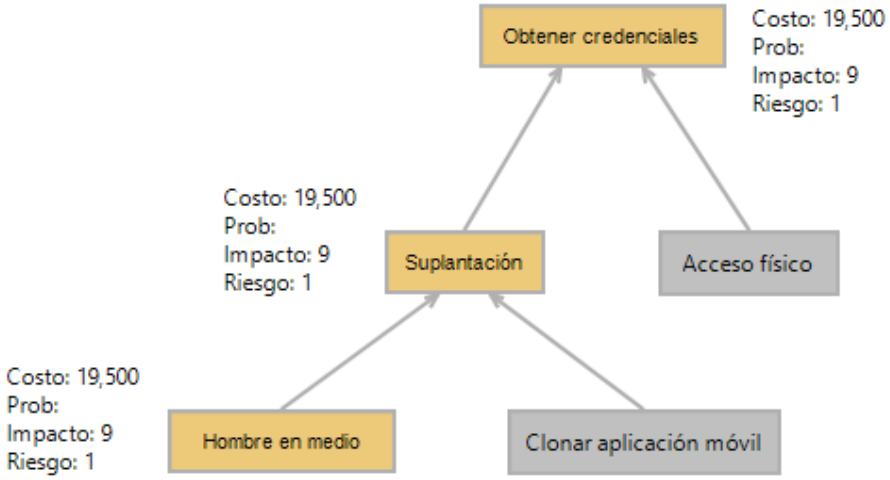


Figura 38. Nodos mitigados por controles (gris) en el árbol de ataque simplificado, cuyo objetivo es la obtención de credenciales de usuario.

Es evidente entonces que, más allá de la intención de cumplir con requisitos regulatorios, las instituciones financieras deben reconocer y darle a las actividades educativas y de difusión el valor que sus beneficios potenciales sugieren.

# Conclusiones

A raíz de los análisis realizados en el desarrollo de este trabajo puede observarse con claridad que, a pesar de la tecnología, la regulación y la difusión, la ocurrencia de ataques mediante código malicioso y hombre en medio sigue siendo una amenaza mayor, debida principalmente a la colaboración inadvertida de los usuarios a través de las diversas plataformas en las que éstos pueden realizar transacciones en la actualidad.

El cada vez más presente paradigma móvil, si bien permite la provisión de nuevos servicios y facilita la interacción con otros ya existentes, de igual manera establece una nueva y amplia superficie de ataque a la que, dado que es asociada con mayor frecuencia a los riesgos de un teléfono y no a aquellos de un dispositivo de cómputo completo, los usuarios aún no han ligado las ideas de vulnerabilidad y de precaución en pos de la seguridad de su información, que con esfuerzo y tiempo se han logrado introducir en lo referente a las computadoras personales clásicas.

Considerando lo anterior, es probable que todas las posibles medidas para mitigar los riesgos previamente identificados deban caer en dos categorías: restringir en los usuarios el poder de tomar decisiones respecto a su seguridad mediante el desarrollo de dispositivos/infraestructura que los protejan efectivamente de ataques relacionados con la ingeniería social, o mejorar e intensificar las labores de difusión y concientización en ellos para que puedan tomar tales decisiones de la mejor manera.

Una de las mejores aproximaciones técnicas al problema ha consistido en la solicitud de múltiples factores de autenticación distribuidos por canales de comunicación fuera de banda, buscando que a pesar de que un equipo se encuentre comprometido, el atacante requiera un elemento extra ajeno al entorno que ya controla. Sin embargo, la sofisticación de las acciones ofensivas en la actualidad es tal que ya contemplan el robo de estos factores adicionales y, más aún, uno de sus medios de distribución más frecuentemente utilizados, los dispositivos móviles, ya alojan las aplicaciones necesarias para la realización de transacciones, por tanto, al contar con sistema y factor adicional en el mismo equipo se pierde el concepto de "fuera de banda."

Un ejemplo ilustrativo es la reciente introducción de lectores biométricos en dispositivos móviles que, a pesar de que en la actualidad únicamente son utilizados para administrar el control de acceso a los equipos y como segundo factor de autenticación en transacciones de muy baja cuantía, a mediano plazo probablemente estarán asociados a un gran número de servicios, sin embargo, una pieza de código malicioso presente en el dispositivo puede obtener una versión digitalizada de una huella digital o de un rostro, la cual puede ser manipulada de la misma manera que una contraseña robada.

Buscando atender lo anterior, se han generado propuestas que trasladan los controles de seguridad de los dispositivos de propósito general hacia otros totalmente dedicados y externos [15, p. 53], los cuales establecen que su utilización en un entorno comprometido por atacantes es posible, ya que generan un canal de comunicación privado entre el propio dispositivo y las instituciones financieras a través de protocolos de comunicación ad-hoc y mensajes estructurados de manera personalizada, además de que toda sesión es enteramente manipulada por el hardware externo, una vez que el usuario a ingresado sus credenciales de banca electrónica exitosamente.

El problema con esta idea radica en que la seguridad del canal de comunicación entre los dispositivos y el banco está basada en la confidencialidad de un secreto previamente

compartido entre ambos participantes (alojado tanto en las unidades externas como en los servidores bancarios), por lo que si la misma pieza de código malicioso que logró el compromiso de la computadora personal/dispositivo móvil del usuario es capaz de ingresar al hardware externo, el secreto compartido puede ser vulnerado y el usuario quedaría expuesto a una variación más del ataque de hombre en medio.

Una alternativa es la adición de un Módulo de Plataforma confiable (TPM, por sus siglas en inglés), que es un hardware dedicado cuya principal función es asegurar la integridad de una plataforma de cómputo, sin limitarse a computadoras personales o a sistemas operativos específicos, desde su arranque en condiciones confiables predeterminadas hasta que los programas controladores han cargado por completo. Esto es logrado a través de la generación y comparación de métricas de seguridad y del cálculo de un valor hash que considera tanto hardware como software, detectando cambios respecto a configuraciones anteriores y tomando decisiones al respecto. Adicionalmente, cuenta con una clave RSA directamente grabada en hardware en el momento de fabricación, a través de la cual pueden generarse conjuntos de llaves asimétricas (sustituyendo el secreto compartido mencionado en el párrafo anterior) o ser utilizada como la parte privada de uno de tales pares. Esta manera de complementar las ideas anteriores, si bien no imposibilitaría el compromiso de los dispositivos externos dedicados, sí evitaría la realización de fraudes debido a que cualquier modificación en el estado confiable sería identificada y notificada al usuario.

Otra opción a considerar es la utilización de un "Live CD"[67] para efectuar transacciones a través de la banca electrónica dado que, al ejecutarse un sistema operativo en memoria RAM, toda la sesión (datos, galletas informáticas, historiales, configuraciones, etc.) es borrada en cuanto deja de proveerse energía eléctrica. Adicionalmente, el omitir la carga de información contenida en el disco duro anfitrión permite prevenir la ejecución de algún tipo de código malicioso presente en él, manteniendo la salud del entorno desde donde se acceden a los servicios financieros en un nivel razonablemente alto.

Un resultado similar podría alcanzarse mediante máquinas virtuales, dado que éstas se encuentran aisladas del sistema operativo en el que corren, sin embargo, para acceder a ellas es indispensable la utilización del disco duro local que, como ya se ha mencionado, puede encontrarse comprometido. Siendo así, no puede asegurarse que a corto o mediano plazo alguna vulnerabilidad en los programas administradores de máquinas virtuales sea descubierta y, por tanto, la integridad de tales entornos separados se vea amenazada.

La implementación de soluciones de estas características se reflejaría en el árbol de ataque original, referente a banca electrónica, anulando todas las ramas relacionadas con la ingeniería social y el código malicioso, dejando la compra de credenciales de acceso en el mercado negro como el único vector de ataque realizable, con una probabilidad de alrededor de 0.15 y un costo hasta 13,000 pesos (Figura 39.) Tales métricas son ligeramente inferiores (5%) a las obtenidas en el escenario ideal de concientización absoluta.

[67] Disco compacto, de sólo lectura, desde el que puede arrancarse un sistema operativo que corre en la memoria de la computadora anfitriona, en lugar de utilizar su disco duro.

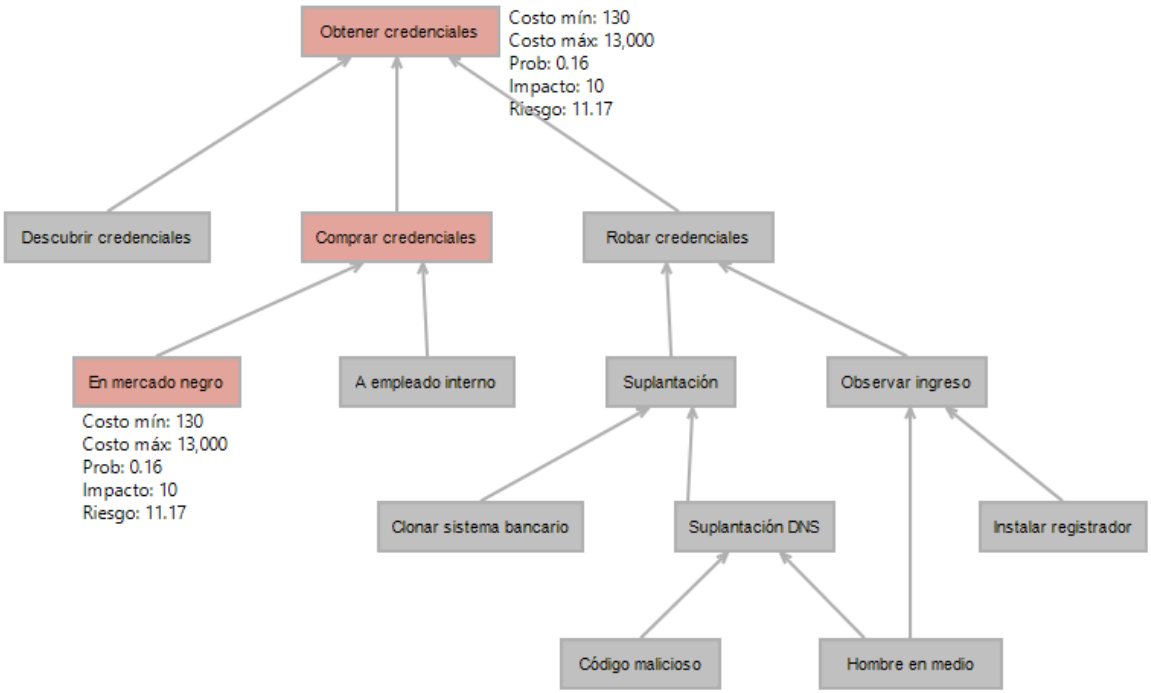


Figura 39. Nodos mitigados por dispositivo dedicado externo (gris) en el árbol de ataque simplificado, cuyo objetivo es la obtención de credenciales de usuario.

En el caso de los dispositivos móviles, el hardware dedicado descrito no puede ser utilizado, ya que su diseño obliga al uso de un navegador web que, como se mencionó anteriormente, no es considerado una forma de banca móvil. Una alternativa para mitigar el hecho de realizar transacciones en plataformas de propósito general, es la de agregar el mencionado chip TPM a los equipos, buscando al menos la detección de modificaciones en los sistemas a través de código malicioso.

Llegando a este punto, sin embargo, nos encontramos nuevamente con una idea presentada con anterioridad: en la actualidad, algunas instituciones consideran más rentable el resarcir económicamente las consecuencias de un fraude a sus clientes que investigar la causa de raíz. Siendo así, luce altamente complicado que se tenga el deseo de invertir en dispositivos tan especializados para cada uno de sus cuentahabientes, por lo que la implementación de este tipo de solución técnica no luce completamente viable. Adicionalmente, dado que el enfoque de este trabajo son los dispositivos móviles, la utilización de un "Live CD" lamentablemente no es aplicable.

Por otro lado, en cuanto a la perspectiva de toma de decisiones informadas, una agresiva iniciativa de difusión y concientización, si bien igualmente acarrearía una elevación de los gastos en las instituciones, a mediano y largo plazo puede arrojar grandes dividendos.

En la actualidad, varias de las actividades de este tipo se encuentran limitadas al cumplimiento mínimo necesario para evitar sanciones regulatorias, lo que aunado al hecho de la hasta ahora baja incidencia en México de fraudes por medios electrónicos, hace parecer que una mayor inversión de tiempo y dinero en estas temáticas no sólo es innecesaria, sino hasta absurda.

Sin embargo, nada puede asegurar que la cantidad de actividades delictuosas mantenga esos niveles mínimos de manera permanente: se han presentado casos muy

recientes (año 2012) de ataques dedicados a instituciones financieras a lo largo de continentes completos que, sustrayendo montos de entre 500 y 250,000 euros por cliente, han alcanzado ganancias de más de 36 millones [47]. Sólo se necesita una brecha para sufrir serios impactos económicos y sanciones regulatorias, así como para sufrir un gran daño en la reputación de las instituciones y sus servicios.

¿Por qué esperar entonces a que los costos por fraude pasen de 100 mil pesos a 36 millones de euros? ¿Por qué no dar mayor importancia a las acciones preventivas, de forma complementaria a las correctivas?

De manera interna las instituciones bancarias, entre muchas otras, establecen dentro de los requerimientos contractuales para todos sus empleados la realización periódica de cursos y evaluaciones en línea. Tales actividades generalmente se encuentran ligadas a cada número de empleado y, cuando no son cumplidas en tiempo y forma, suelen desembocar en acciones disciplinarias que en última instancia pueden significar rescisiones de contrato o hasta acciones legales.

Una aproximación similar podría ser aplicada en el contexto de la banca electrónica cuando un cuentahabiente solicite la prestación de tales servicios. Esta idea puede ser abordada desde tres perspectivas diferentes: la informativa, en la que se busque dejar claro al usuario el potencial beneficio de la realización de un curso, evaluación y revalidación anual en línea, la contractual, en la que se ligue la prestación del servicio a las actividades antes descritas y la regulatoria, que complemente las disposiciones de las diferentes entidades, en lo referente a los servicios por medios electrónicos.

Como ya se mencionó en capítulos anteriores, cada vez son más los usuarios que consideran que la seguridad de su información es una responsabilidad compartida con las instituciones de las que son clientes. Siendo así, la correcta exposición de los motivos detrás de la aplicación de un curso gratuito, con duración de entre 30 y 40 minutos, con evaluación que, de no ser acreditada, exija la repetición del curso y de actualización anual, en conjunto con una obligación contractual que desmotive al usuario de delegar la realización de estas actividades, podría ser un buen inicio en pos de una concientización más generalizada.

Del lado de las instituciones, la aplicación de este tipo de medidas requeriría la revisión de infraestructura ya existente para el uso de sus empleados, su ampliación de ser necesaria, la evaluación y atención de los nuevos riesgos que esta superficie de ataque adicional supondrían y, por supuesto, la inclusión de toda esta idea dentro de sus procesos administrativos y planes de negocio, actividad que igualmente se debe realizar con la inclusión de los nuevos servicios que originan todo el análisis. Adicionalmente se requeriría la adopción de criterios comunes entre todas las instituciones, como ya se hace con acuerdos internaciones de regulación financiera, para evitar que el usuario, con tal de evitar estas disposiciones, acuda a aquél que ofrezca los servicios electrónicos sin ningún tipo de exigencia adicional.

El beneficio potencial de esta aproximación ya fue analizado en los capítulos 4 y 6 de este trabajo.

## Consideraciones finales

El desarrollo del presente trabajo se encontró principalmente con dos obstáculos: la dificultad de obtener información sobre los procesos e infraestructuras bancarios y la

dificultad para calcular o inferir métricas para los árboles de ataque a través de la información disponible.

Por razones evidentes, las instituciones bancarias desarrollan sus actividades en ambientes altamente controlados y restrictivos donde, además de los activos monetarios transaccionados diariamente, la información es un bien crítico.

Como parte de sus disposiciones más básicas, las políticas internas de seguridad de estas entidades establecen criterios muy específicos para clasificar la información en base a potenciales riesgos que su divulgación no autorizada provocaría, otorgando comúnmente a los diagramas de infraestructura, configuraciones de seguridad y reportes de vulnerabilidades los niveles más altos. Siendo así, aún para personal interno, el acceder a cierto tipo de información no es sencillo.

Por otro lado, la obtención de métricas adecuadas para el análisis del riesgo se limita básicamente a dos alternativas, el recurrir a información ya existente, disponible en diversas fuentes (artículos, trabajos académicos de investigación, informes anuales por parte de instituciones o empresas especializadas, etc.), o generarlas de manera personal.

Una posibilidad para lograr lo anterior puede ser a través de la realización de una encuesta, sin embargo, el conjuntar una muestra representativa de responsables de seguridad dispuestos a proveer información que, como se mencionó anteriormente, suele ser altamente restringida, luce muy complicado. Adicionalmente, un ejercicio de tal magnitud potencial puede ser considerado en algunos casos como una investigación con méritos suficientes para ser tratada de manera individual y no como una mera actividad complementaria al servicio de otros objetivos.

Siendo así, se optó por la recopilación de una gran cantidad de datos que, en última instancia, permitieran aproximar valores adecuados para caracterizar cada nodo de las estructuras de árbol propuestas, sin embargo, la generalidad de la información obtenida provocó que ramas previamente desarrolladas a gran detalle tuvieran que ser adaptadas y reducidas de acuerdo a las estadísticas con las que se contaba, dejando de considerar una gama más amplia de ataques y manteniendo conceptos más genéricos.

Lo anterior da la pauta para discutir con mayor detalle lo que el uso de la metodología seleccionada logró aportar, evaluando así si los objetivos planteados originalmente fueron cubiertos a cabalidad.

Analizando los árboles de ataque desde una perspectiva puramente teórica, puede vislumbrarse una alternativa sumamente completa para la realización de análisis de riesgos, debido a la posibilidad de modelar gráfica y metódicamente amenazas y vulnerabilidades, así como de caracterizarlas para su posterior estudio.

La correcta construcción de una estructura de este tipo facilita la toma de decisiones de seguridad al tener un panorama muy amplio de la problemática a la que el sistema analizado se encuentra expuesto, sin embargo, este ejercicio no es trivial en absoluto.

En primer lugar se tiene la desventaja de que el modelo sólo puede incluir ataques conocidos por aquel que lo genera, por lo que el resultado final es directamente proporcional a los conocimientos y/o experiencia del analista. Por otro lado, de manera irónica, un nivel de detalle muy profundo igualmente puede producir grandes inconvenientes al hacer crecer el análisis en extensión y complejidad, así como dificultar el establecimiento de las métricas adecuadas.

Por lo tanto, la adopción práctica de una metodología como esta podría depender quizá del establecimiento de un nivel de detalle medio que, sin una granularidad tan fina, refleje fielmente los procesos más críticos de un sistema y las amenazas a los que éstos están expuestos. De manera adicional, el concentrado en una base de datos de los valores de diversas métricas, actualizados de manera constante, agilizaría en gran medida el proceso de generación de la estructura y, en consecuencia del análisis completo.

Habiendo establecido todo lo anterior, surge la interrogante principal: ¿La búsqueda del cumplimiento de los objetivos de este trabajo mediante árboles de ataque resultó ser una elección adecuada? ¿Tales objetivos fueron finalmente alcanzados?

La meta originalmente establecida consistía en analizar si los controles de seguridad actualmente implementados en los principales servicios de banca a través de internet y móvil eran los suficientes y, de ser necesario, proponer medidas preventivas adicionales que mitigaran riesgos residuales y sus posibles impactos.

La perspectiva provista por los árboles construidos para cada servicio permitió identificar que, si bien éstos tienen establecidos una gran cantidad de controles tecnológicos y regulatorios, al final de día gran parte de la responsabilidad por la ocurrencia de fraudes recae en los usuarios (elección de una metodología adecuada), para cuyas acciones muy pocos controles significativos están contemplados (determinación de la insuficiencia de los controles.)

Una vez identificada una problemática concreta, se propusieron alternativas tanto técnicas como regulatorias y de difusión para atenderla (propuesta de medidas adicionales), evidenciando a la vez su utilidad a través de la variación positiva en las métricas de los árboles construidos (mitigación de riesgos residuales), quedando entonces cubiertas todas las interrogantes planteadas.

## Trabajo futuro

En lo referente a la metodología, un mayor detalle en la construcción de los árboles, considerando una gama más amplia de ataques y métricas adicionales, permitiría la obtención de resultados más exactos y variados que, en consecuencia, aportarían un mayor nivel de visibilidad para los encargados de tomar decisiones de seguridad en base a análisis de riesgos.

En cuanto a las propuestas de mitigación realizadas, un punto a considerar puede ser la construcción y desarrollo de las soluciones técnicas descritas, así como la experimentación con éstas para confrontar su efectividad y aceptación reales con los resultados del análisis teórico desarrollado a lo largo de los capítulos del presente trabajo.

# Referencias


[1] A. Chovanová, «Forms of Electronic Banking,» *BIATEC Banking Journal,* vol. 14, nº 6, pp. 22-25, 2006.

[2] Asociación Mexicana de Internet, «Banca Electrónica 2012,» 2012.

[3] J. Bowen, «How ATMs Work,» HowStuffWorks, 2000 Abril 1. [En línea]. Available: http://money.howstuffworks.com/personal-finance/banking/atm.htm. [Último acceso: 2013 Julio 1].

[4] V. Flores Tantaleán, «Comercio electrónico: Emagister,» Grupo Intercom, 23 Abril 2010. [En línea]. Available: http://www.emagister.com/curso-comercio-electronico-business-3-3/banca-electronica. [Último acceso: 24 Abril 2013].

[5] S. Nsouli y A. Schaechter, «Challenges of the "E-Banking Revolution",» *Finance & Development, A Quarterly Magazine of the International Monetary Fund,* vol. 39, nº 3, 2002.

[6] K. C. Laudon y C. Guercio Traver, E-commerce: Business, Technology, Society, Octava ed., Nueva Jersey: Prentice Hall, 2012.

[7] J. Claessens, V. Dem, D. De Cock, B. Preneel y J. Vandewalle, «On the Security of Today's Online Electronic Banking Systems,» *Computers & Security,* vol. 21, nº 3, pp. 257-269, 2002.

[8] Panda Security Press, «Malware Creation hit a New Record High in 2011 with 26 million samples,» 31 Enero 2012. [En línea]. Available: http://press.pandasecurity.com/news/malware-creation-hit-a-new-record-high-in-2011-with-26-million-samples/. [Último acceso: 15 Mayo 2013].

[9] Panda Security Press, «PandaLabs Q1 Report: Four Out Of Five New Malware Samples Are Trojans,» 7 Mayo 2012. [En línea]. Available: http://press.pandasecurity.com/news/pandalabs-q1-report-four-out-of-five-new-malware-samples-are-trojans/. [Último acceso: 15 Mayo 2013].

[10] Laboratorio de ESET Latinoamérica, «Tendencias 2011: las botnet y el malware dinámico,» ESET Latinoamérica, Buenos Aires, 2010.

[11] J. Guilfoyle, «Symantec Report on the Underground Economy - Spokesperson Training,» Symantec, 2009.

[12] Symantec Corporation, «Internet Security Threat Report 2011,» Symantec, Mountain View, 2011.

[13] OWASP, «Top 10 2013,» OWASP Foundation, 4 Julio 2013. [En línea]. Available: https://www.owasp.org/index.php/Top_10_2013. [Último acceso: 29 Julio 2013].

[14] Computer Security Institute, «15th Annual 2010/2011 Computer Crime and Security Survey,» Computer Security Institute, Nueva York, 2011.

[15] M. Johnson, «A new approach to Internet banking,» University of Cambridge, Cambridge, 2008.

[16] Enterasys Networks, «Understanding Network Access Control,» Enterasys Networks, 2009.

[17] Verisign, «DDoS and Downtime: Considerations for Risk Management,» Verisign Inc., 2012.

[18] Basel Committee on Banking Supervision, «Risk Management Principles for Electronic Banking,» Bank for International Settlements, Basilea, 2003.

[19] R. Stephans, System Safety for the 21st Century, The Updated and Revised Edition of System Safety 2000, Hoboken, Nueva Jersey: Wiley-Interscience, 2004.

[20] ISO/IEC, *Estándar Internacional ISO/IEC 27001:2005,* 1.0 ed., ISO/IEC, 2005.

[21] C. Alberts y A. Dorofee, «OCTAVE Criteria, Version 2.0,» Carnegie Mellon University, Pittsburgh, 2001.

[22] National Institute of Standards and Technology, «Managing Information Security Risk. Organization, Mission, and Information System View,» Gaithersburg, 2011.

[23] L. Marín y C. Velásquez, *Metodología de Identificación de Peligros, Evaluación y Control de Riesgos,* Consejo Colombiano de Seguridad, 2004.

[24] E. Hayden, «How to determine the net value of an asset for risk impact analysis,» TechTarget, Mayo 2010. [En línea]. Available: http://searchsecurity.techtarget.com/answer/How-to-determine-the-net-value-of-an-asset-for-risk-impact-analysis. [Último acceso: 30 Junio 2013].

[25] Intangible Business, «How to Value Intangible Assets,» Intangible Business, Abril 2008. [En línea]. Available: http://www.intangiblebusiness.us/news/financial/2008/04/how-to-value-intangible-assets. [Último acceso: 30 Junio 2013].

[26] J. d. J. Vázquez, «Administración de Riesgos y Continuidad de Operaciones,» de *Diplomado en Seguridad de la Información, Edición 24*, Ciudad de México, 2012.

[27] J. Dugan, «Fault Tree Analysis of Computer-Based Systems,» de *Reliability and Maintainability Symposium*.

[28] C. Ericson II, *Fault Tree Analysis,* 2000.

[29] B. Schneier, «Attack Trees,» *Dr. Dobb's Journal,* vol. 24, nº 12, Diciembre 1999.

[30] P. L. Clemens, *Event Tree Analysis,* Sverdrup, 1990.

[31] B. Schneier, «Attack Trees,» de *SANS Network Security 99*, Nueva Orleans, 1999.

[32] K. Edge, R. Raines, M. Grimalia, R. Baldwin, R. Bennington y C. Reuter, «The Use of Attack and Protection Trees to Analize Securirty for an Online Banking System,» de *Proceedings of the 40th Hawaii International Conference on System Sciences*, Hawaii, 2007.

[33] BBVA, «La banca móvil en México como mecanismo de inclusión financiera: desarrollos recientes y aproximación al mercado potencial,» BBVA Research, México, D.F., 2013.

[34] CIFAS, «Staff Fraudscape. Depicting the UK's fraud landscape,» CIFAS, Londres, 2013.

[35] Fortinet, «Fortinet 2013 Cybercrime Report,» 2013.

[36] Get Cyber Safe, «Phishing: How many take the bait?,» Government of Canada, 31 Julio 2013. [En línea]. Available: http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspx. [Último acceso: 16 Septiembre 2013].

[37] A. Schaap, «Characterization of Tor Exit-Nodes,» de *18th Twente Student Conference on IT* , Twente, 2013.

[38] N. McAllister, «Tor usage up by more than 100% in August,» The Register, 29 Agosto 2013. [En línea]. Available: http://www.theregister.co.uk/2013/08/29/tor_usage_up_by_more_than_100_in_august/. [Último acceso: 3 Marzo 2014].

[39] K. N. Gopinath y H. Chaskar, «All You Wanted to Know About WiFi Rogue Access Points,» AirTight Networks, 2009.

[40] Trustwave, «2013 Global Security Report,» Trustwave Holdings Inc., Chicago, 2013.

[41] Cyveillance, «Malware Detection Rates for Leading AV Solutions,» 2010.

[42] P. Royal, «Maliciousness in Top-ranked Alexa Domains,» Barracuda Labs, 28 Marzo 2012. [En línea]. Available: http://barracudalabs.com/2012/03/maliciousness-in-top-ranked-alexa-domains/. [Último acceso: 2013 Septiembre 17].

[43] WhiteHat Security, «Website Security Statistics Report,» 2013.

[44] Central Intelligence Agency, «The World Factbook 2012-2013,» Washington, DC, 2012.

[45] J. Mick, «Wrath of the Titans: Microsoft, U.S. Feds Slay Godly "Zeus" Botnets,» DailyTech LLC, 26 Marzo 2012. [En línea]. Available: http://www.dailytech.com/Wrath+of+the+Titans+Microsoft+US+Feds+Slay+Godly+Zeus+Botnets/article24306.htm. [Último acceso: 17 Septiembre 2013].

[46] Verizon, «2013 Data Breach Investigations Report,» Verizon, 2013.

[47] E. Kalige y D. Burkey, «A Case Study of Eurograbber: How 36 Million Euros was Stolen via Malware,» Versafe Secure Login; Check Point Software Technologies LTD., 2012.

[48] Trusteer, «Acerca de Rapport,» Trusteer, 2013. [En línea]. Available: http://www.trusteer.com/es/support/about-rapport. [Último acceso: 6 Octubre 2013].

[49] N. Kettle, «Unbiased Review of Trusteer Rapport,» de *44CON*, Londres, 2011.

[50] N. Kettle, «Trusteer 'respond' to Rapport Issues,» Digit Security Ltd, 12 Octubre 2011. [En línea]. Available: http://www.digit-security.com/blog/?p=333. [Último acceso: 6 Octubre 2013].

[51] J. Leyden, «REVEALED: Cyberthug tool that BREAKS HSBC's anti-Trojan tech,» The Register, 6 Agosto 2013. [En línea]. Available: http://www.theregister.co.uk/2013/08/06/trusteer_pushes_updates_after_cybercrook_brew_up_browser_lockdown_exploit/. [Último acceso: 6 Octubre 2013].

[52] C. Williams, «Zeus Botnet Impersonating Trusteer Rapport Update,» Cisco, 19 Julio 2013. [En línea]. Available: http://blogs.cisco.com/security/zeus-botnet-impersonating-trusteer-rapport-update/. [Último acceso: 6 Octubre 2013].

[53] Banamex, «Herramienta Anti-Intrusos,» Grupo Financiero Banamex, 2011. [En línea]. Available: https://boveda.banamex.com.mx/spanishdir/ayudas/masinfoahnlab.htm. [Último acceso: 6 Octubre 2013].

[54] Ahnlab, «AOS (AhnLab Online Security),» AhnLab, Inc., [En línea]. Available: http://global.ahnlab.com/en/site/product/productSubDetail.do?prod_type=P1&prod_class=P&prod_seq=9008. [Último acceso: 6 Octubre 2013].

[55] CVE, «Ahnlab V3 Internet Security: Security Vulnerabilities (Bypass),» MITRE Corporation, [En línea]. Available: http://www.cvedetails.com/vulnerability-list/vendor_id-3339/product_id-12594/opbyp-1/Ahnlab-V3-Internet-Security.html. [Último acceso: 6 Octubre 2013].

[56] V. M. Alba, «Cybercrimen en la Banca en México,» de *8a Semana de la Seguridad Informática*, Ciudad de México, 2013.

[57] Gartner, «Gartner Says Worldwide PC, Tablet and Mobile Phone Shipments to Grow 5.9 Percent in 2013 as Anytime-Anywhere-Computing Drives Buyer Behavior,» Gartner, 24 Junio 2013. [En línea]. Available: http://www.gartner.com/newsroom/id/2525515. [Último acceso: 28 Agosto 2013].

[58] Gartner, «Gartner Says Smartphone Sales Grew 46.5 Percent in Second Quarter of 2013 and Exceeded Feature Phone Sales for First Time,» Gartner, 14 Agosto 2013. [En línea]. Available: http://www.gartner.com/newsroom/id/2573415. [Último acceso: 28 Agosto 2013].

[59] C. Marmolejo, «Banca Móvil: potencial crecimiento y protección del consumidor en México,» 2009.

[60] comScore, «2011 State of Online and Mobile Banking,» comScore, 2012.

[61] INEGI; CNBV, «Encuesta Nacional de Inclusión Financiera,» 2012.

[62] Google, «Our Mobile Planet: México,» Ipsos OTX MediaCT, 2012.

[63] The Competitive Intelligence Unit, «Para el 2015, con smartphone 7 de cada 10 usuarios de celular,» The Competitive Intelligence Group, 26 Enero 2012. [En línea]. Available: http://www.the-ciu.net/. [Último acceso: 29 Agosto 2013].

[64] Subdirección de Seguridad de la Información, «Malware móvil aumenta 163%,» 17 Abril 2013. [En línea]. Available: http://www.seguridad.unam.mx/noticia/?noti=981. [Último acceso: 15 Mayo 2013].

[65] D. Gross, «¿Estás seguro que tu iPhone está libre de 'malware'? Quizá no tanto.,» CNN México., 3 Junio 2013. [En línea]. Available: http://mexico.cnn.com/tecnologia/2013/06/03/estas-seguro-que-tu-iphone-esta-libre-de-malware-quiza-no-tanto. [Último acceso: 2013 Octubre 27].

[66] A. Heyman, «First SpyEye Attack on Android Mobile Platform Now in the Wild,» Trusteer, 13 Septiembre 2011. [En línea]. Available: http://www.trusteer.com/blog/first-spyeye-attack-android-mobile-platform-now-wild. [Último acceso: 28 Octubre 2013].

[67] A. Greenberg, «iOS 7 Bug Lets Anyone Bypass iPhone's Lockscreen To Hijack Photos, Email, Or Twitter,» Forbes.com LLC, 19 Septiembre 2013. [En línea]. Available: http://www.forbes.com/sites/andygreenberg/2013/09/19/ios-7-bug-lets-anyone-bypass-iphones-lockscreen-to-hijack-photos-email-or-twitter/. [Último acceso: 28 Octubre 2013].

[68] J. Kirk, «Old tricks help German hackers bypass iPhone 5s Touch ID security,» IDG Consumer & SMB, 23 Septiembre 2013. [En línea]. Available: http://www.macworld.com/article/2049221/old-tricks-help-german-hackers-bypass-iphone-5s-touch-id-security.html. [Último acceso: 28 Octubre 2013].

[69] M. Kumar, «Android vulnerability allows hackers to modify apps without breaking signatures,» The Hacker News, 4 Julio 2013. [En línea]. Available: http://thehackernews.com/2013/07/android-vulnerability-allows-hackers-to.html. [Último acceso: 28 Octubre 2013].

[70] K. Zetter, «Hacker Spoofs Cell Phone Tower to Intercept Calls,» Wired.com, 31 Julio 2010. [En línea]. Available: http://www.wired.com/threatlevel/2010/07/intercepting-cell-phone-calls/. [Último acceso: 24 Octubre 2013].

[71] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon y R. Borgaonkar, *New Privacy Issues in Mobile Telephony: Fix and Verification,* 2012.

[72] A. Goujon, «¿Qué conexión es más segura, 3G o Wi-Fi?,» ESET Latinoamérica, 24 Octubre 2013. [En línea]. Available: http://blogs.eset-la.com/laboratorio/2013/10/24/conexion-mas-segura-3g-wi-fi/. [Último acceso: 28 Octubre 2013].

[73] S. Kolesnikov-Jessop, «Hackers Go After the Smartphone,» 13 Febrero 2011. [En línea]. Available: http://www.nytimes.com/2011/02/14/technology/14iht-srprivacy14.html. [Último acceso: 15 Mayo 2013].

[74] E. Messmer, «Apple iPhones, iPads get intrusion-detection and prevention from start-up,» IDG, 17 Octubre 2013. [En línea]. Available: http://www.pcadvisor.co.uk/news/security/3474197/apple-iphones-ipads-get-intrusion-detection-and-prevention-from-start-up/. [Último acceso: 30 Octubre 2013].

[75] S. Malenkovich, «Have no fear, iPad!,» Kaspersky Lab ZAO, 23 Octubre 2013. [En línea]. Available: http://blog.kaspersky.com/have-no-fear-ipad/. [Último acceso: 30 Octubre 2013].

[76] Security Research Labs, «Mobile networks differ widely in security, none protect well in all dimensions,» SRLabs, [En línea]. Available: https://srlabs.de/gsmmap. [Último acceso: 3 Noviembre 2013].

[77] Telsis, «The Case for SMS Home Routing,» Telsis, 2012.

[78] Open Web Application Security Project, «OWASP Mobile Security Project,» Open Web Application Security Project, 22 Mayo 2013. [En línea]. Available: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project. [Último acceso: 3 Noviembre 2013].

[79] R. Brain, «Dynamic code analysis vs. static analysis source code testing,» TechTarget, Septiembre 2010. [En línea]. Available: http://www.computerweekly.com/answer/Dynamic-code-analysis-vs-static-analysis-source-code-testing. [Último acceso: 3 Noviembre 2013].

[80] Apple, «Which Developer Program is for you?,» Apple Inc., 2013. [En línea]. Available: https://developer.apple.com/programs/which-program/. [Último acceso: 18 Noviembre 2013].

[81] S. Tibken, «Google ties Apple with 700,000 Android apps,» CBS Interactive Inc., 30 Octubre 2012. [En línea]. Available: http://news.cnet.com/8301-1035_3-57542502-94/google-ties-apple-with-700000-android-apps/. [Último acceso: 18 Noviembre 2013].

[82] Trend Micro, «TrendLabs 2012 Mobile Threat and Security Roundup,» Trend Micro, 2013.

[83] SMSCaster E-Marketer, «Order SMSCaster E-Marketer Online,» SDJ Software Limited, Agosto 2013. [En línea]. Available: http://www.smscaster.com/ordersmscaster.htm. [Último acceso: 19 Noviembre 2013].

[84] S. Delany, M. Buckley y D. Greene, «SMS spam filtering: Methods and data,» *Expert Systems with Applications,* 2012.

[85] S. Bortnik, «Why do phishing attacks work better on mobile phones?,» ESET, 20 Enero 2011. [En línea]. Available: http://www.welivesecurity.com/2011/01/20/why-do-phishing-attacks-work-better-on-mobile-phones/. [Último acceso: 18 Noviembre 2013].

[86] A. Gahran, «Después de las 9 de la noche aumenta el riesgo de que pierdas tu celular,» CNN México, 27 Marzo 2012. [En línea]. Available: http://mexico.cnn.com/tecnologia/2012/03/27/despues-de-las-9-de-la-noche-aumenta-el-riesgo-de-que-pierdas-tu-celular. [Último acceso: 18 Noviembre 2013].

[87] CVE Details, «Security Vulnerabilities for iPhone OS,» MITRE Corporation, 2013. [En línea]. Available: http://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-15556/Apple-Iphone-Os.html. [Último acceso: 18 Noviembre 2013].

[88] Banamex, «Preguntas Frecuentes,» [En línea]. Available: http://www.banamex.com/es/personas/servicios/banca_electronica/sitio_movil/pdf/FAQs.pdf. [Último acceso: 24 Noviembre 2013].