Instituto Politécnico Nacional

Escuela Superior de
Ingeniería Mecánica y Eléctrica
Unidad Culhuacán

Sección de Estudios de Posgrado e Investigación

Análisis Comparativo de Incidentes en la Aplicación del Voto Electrónico

Tesis
Que para obtener el grado de

Maestría en Ingeniería en Seguridad
y Tecnologías de la Información

Presenta

Lic. Gunnar Eyal Wolf Iszaevich

Asesores:
MSI. Pablo Ramón Mercado Hernández
Dra. Gina Gallegos García

Ciudad de México, abril de 2018

SIP-14-BIS

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de México siendo las 20:00 horas del día 7 del mes de marzo del 2018 se reunieron los miembros de la Comisión Revisora de la Tesis, designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de SEPI-ESIME-CULHUACAN para examinar la tesis titulada:

"Análisis Comparativo de Incidentes en la Aplicación del Voto Electrónico"

Presentada por el alumno:

Wolf	**Iszaevich**	**Gunnar Eyal**
Apellido paterno	Apellido materno	Nombre(s)

Con registro: B 1 5 0 4 8 6

aspirante de:

MAESTRÍA EN INGENIERÍA EN SEGURIDAD INFORMÁTICA Y TECNOLOGÍAS DE LA INFORMACIÓN

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***APROBAR LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Directores de tesis

M. en C. Pablo Ramón Mercado Hernández

Dra. Gina Gallegos García

Dr. Gabriel Sánchez Pérez

Dr. Rogelio Reyes Reyes

Dr. Jesús Arturo Flores López

INSTITUTO POLITECNICO NACIONAL
ESTADOS UNIDOS MEXICANOS
S.E.P.
SECCION DE ESTUDIOS DE POSGRADO E INVESTIGACION
ESIME CULHUACAN

PRESIDENTE DEL COLEGIO DE PROFESORES

Dr. Héctor Manuel Pérez Meana

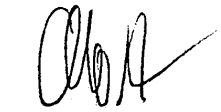
INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la Ciudad de México, el día 20 del mes de marzo del año 2018, el que suscribe **Gunnar Eyal Wolf Iszaevich,** alumno del Programa de **Maestría en Ingeniería en Seguridad y Tecnologías de la Información,** con número de registro **B150486,** adscrito a la **Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán,** manifiesta que es autor intelectual del presente trabajo de Tesis bajo la dirección del **MSI. Pablo Ramón Mercado Hernández** y la **Dra. Gina Gallegos García**, y cede los derechos del trabajo intitulado **Análisis Comparativo de Incidentes en la Aplicación del Voto Electrónico**, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección **gwolf@gwolf.org**. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.



Lic. Gunnar Eyal Wolf Iszaevich

Resumen

Alrededor del mundo, hay muy pocas cosas en que estén de acuerdo los diferentes esquemas bajo los cuales se gobiernan las sociedades humanas; uno los puntos en que hay mayor consenso en el acuerdo es que la democracia –el que las decisiones implementadas para una sociedad sean un reflejo de los intereses del conjunto de sus miembros– es un valor deseado y positivo.

A lo largo de la historia ha habido numerosas maneras de materializar este ideal — De emitir el sufragio, de contabilizarlo y totalizarlo. Desde hace ya más de un siglo existen mecanismos que permiten hacerlo por medios automatizados (en primer término, mecánicos; hoy en día, principalmente computarizados). Hay, sin embargo, una cacofonía de argumentos contradictorios provenientes de todo tipo de disciplinas respecto a la factibilidad, conveniencia y seguridad de dicha automatización.

La presente investigación detalla el análisis de la clasificación, empleando distintas taxonomías orientadas a la seguridad informática, de un conjunto de incidentes derivados de la aplicación de esquemas de voto electrónico, buscando patrones emergentes y características comunes que éstos reflejen, buscando servir como base para la generación de un documento de mejores prácticas que pueda mejorar la seguridad de implementaciones futuras.

Abstract

The different schemes through which human societies are governed throughout the world can rarely be made to agree. One of the most prevalent agreement points is that some understanding of *democracy*, that is, having the implemented decisions for a given society reflect the interests of its members, is a sought and positive value.

Throughout history there have been several ways to materialize this ideal — For individuals to issue a vote and for an electoral entity to add, count and total it. For over a century, there are mechanisms that allow to perform this task by automated means (in the beginning, mechanical; nowadays, mostly computerized). There is, however, a cacophony of contradictory arguments owing to very different disciplines regarding the feasibility, convenience and security of such automation.

This research details the analysis of the classification, using different computer security-oriented taxonomies, of a set of incidents derived from the application of electronic voting systems, in search for emerging patterns and common characteristics reflected in them, and aiming to serve as a basis for generating a best practices document that can help improve the security of future implementations.

Dedicatoria

Para mis padres.

Gracias a Regina.

Por Alan y Elena.

Por todo y por más.

Índice general

Capítulo 1

Introducción

1.1. Definición del problema

Al abordar este tema se hace evidente la contradicción entre diversos trabajos por parte de expertos en disciplinas variadas respecto a la conveniencia (o no) de promover su adopción. Pueden encontrarse numerosos trabajos, bien justificados y argumentados, en ambos casos publicados con todo rigor académico, pero las conclusiones a que llegan son diametralmente opuestas.

Se han hecho numerosas implementaciones que pueden clasificarse como voto electrónico desde hace más de 20 años; algunas de dichas implementaciones han presentado fallos, desde menores hasta severos. Claro está, también ha habido numerosas votaciones electrónicas exitosas. La información técnica disponible respecto a dichas experiencias es, sin embargo, muy limitada.

La idea misma de celebrar votaciones mediante equipos de cómputo ha sido objeto de numerosas controversias. La votación electrónica puede abordarse desde muy distintos ángulos: Desde las ciencias sociales, hay numerosos ángulos legales y sociológicos. El presente trabajo se presenta desde el campo de la ingeniería, particularmente de la seguridad informática; en éste, puede abordarse a partir de distintos aspectos: Matemático, analizando los algoritmos criptográficos empleados para cada etapa del proceso; de ingeniería de software, enfocándose en las prácticas seguidas para el desarrollo de su software; de seguridad informática, revisando la robustez de los modelos de componentes, la seguridad en las comunicaciones, etcétera. Y si bien en muchos de estos campos por separado parece haber respuestas claras y definitivas indicando que sí es posible desarrollar esquemas seguros para sustentar una votación electrónica, los análisis que integran a dichos campos, hechos a mayor distancia, arrojan resultados mayormente negativos.

Por tanto, el problema de partida de este trabajo es: De las implementaciones que se han registrado de voto electrónico, pueden encontrarse casos de éxito — y casos de fallo. Dada la carencia de una sistematización en la información relativa a dichos fallos, las nuevas implementaciones que se siguen desarrollando muchas veces caen en los mismos problemas que ya se habían presentado.

1.2. Objetivo general

Evaluar el uso de distintas taxonomías orientadas a la seguridad informática, basados en el análisis de un conjunto de incidentes observados en casos de estudio de implementaciones de voto electrónico, para la identificación de problemas comunes y recomendaciones tendientes a la multidisciplinariedad en el diseño de

este tipo de sistemas.

1.3. Objetivos particulares

1. Identificar un conjunto de casos de incidentes relacionados con la aplicación del voto electrónico
2. Seleccionar taxonomías de fallos o vulnerabilidades informáticas relevantes para la clasificación de los casos de incidentes
   a) Comparar y elegir las taxonomías más relevantes para el espacio problematizado
3. Clasificar los casos de incidentes según las taxonomías elegidas
   a) Diagramar individualmente los resultados de la clasificación de forma homogénea y comparable
   b) Integrar, diagramar e interpretar el conjunto de datos como un todo para cada una de las taxonomías
4. Contrastar modelos de madurez relevantes a la seguridad informática susceptibles de ser aplicados ante los problemas estudiados
5. Evaluar los modelos de madurez abordados de cara a la información obtenida de la aplicación de las taxonomías

1.4. Hipótesis

Si bien la implementación del voto electrónico *parece estar* dentro de los alcances de diversas disciplinas, su complejidad se desprende de ser un problema *profundamente transdisciplinario*.

Las respuestas parciales a problemáticas observadas, e incluso el mismo análisis que se les puede hacer desde la perspectiva de la seguridad de la información, escapan de la complejidad de este proceso y resultan insuficientes para describir siquiera los problemas a suficiente detalle.

Este trabajo se desarrolla a partir de la hipótesis de que, si se parte de la caracterización de un conjunto de casos en que se compromete alguna de las propiedades que persigue la implementación de esquemas de voto electrónico, se pueden encontrar características comunes que contribuyan a comprender mejor los detalles al hacer análisis integrales.

1.5. Justificación

Hablar de seguridad informática de forma monolítica es imposible. La cantidad de áreas del conocimiento que la conforman, así como de ángulos desde los cuales éstas pueden abordarse. Las disciplinas pueden y deben cruzarse, y la evaluación integral de seguridad de un sistema cuya aplicación tiene profundas implicaciones sociales no puede limitarse a una comprensión parcial de la realidad.

Analizar la seguridad de los esquemas de voto electrónico ilustra muy bien esta problemática: Si bien existen numerosos trabajos presentando las distintas *piezas del rompecabezas* con todo rigor matemático y metodológico, y si bien estas son aparentemente respaldadas por sendas justificaciones desde el punto de vista sociopolítico, una adecuada implementación de dichos procedimientos resulta prácticamente imposible.

El presente trabajo busca abonar a esta discusión integrando una evaluación cubriendo distintos enfoques previamente validados, encontrando patrones que emerjan transversalmente de los varios casos; esta evaluación puede ayudar a la integración de marcos de prueba, manuales de mejores prácticas y demás.

Este trabajo presenta las áreas en que se concentran los factores causales de los fallos observados; pueden tomarse como tal, o puede seguirse la metodología desarrollada con otro conjunto de fallos y comparar que los resultados sigan el mismo comportamiento.

Capítulo 2

Marco teórico

2.1. Objetivos de la seguridad de la información

Un sistema de información puede implementarse siguiendo distintos criterios; al evaluar al problema del voto electrónico desde el ámbito de la seguridad de la información, uno de los primeros puntos en que debe enfocarse la atención es en cuáles *objetivos* o *propiedades de la seguridad de la información* (Menezes, Van Oorschot y Vanstone 1996, pág. 4) resultan más relevantes.

Diferentes autores han analizado este planteamiento; tanto el modelo planteado por Tjøstheim, Peacock y Ryan 2007 como la definición que forma parte de FISMA (107th Congress of the United States of America 2002, Tit. III § 3542(b)(1)) están sustentados en tres aspectos centrales, *integridad, confidencialidad y disponibilidad*. A continuación, se presentan estos aspectos de fundamental importancia desde el significado que adquieren en el contexto de los sistemas electorales; cada uno de ellos se acompaña de la definición del *objetivo de seguridad* correspondiente conforme Menezes, Van Oorschot y Vanstone 1996.

Integridad Los votos se emiten siguiendo la voluntad de su respectivo votante; los votos son contados en el mismo sentido que fueron emitidos. De estos dos postulados sigue que el resultado representa a la voluntad del conjunto de votantes.

Asegurar que la información no ha sido alterada por medios no autorizados o desconocidos.

Confidencialidad El sentido del voto de cada uno de los votantes debe ser imposible de averiguar o recuperar. No únicamente debe protegerse este dato ante terceros interesados, sino que incluso ante el mismo votante[1].

Mantener la información secreta de todos, a excepción de aquellos autorizados para verla.

Autenticación Únicamente debe permitírsele emitir un voto a los votantes autorizados.

Corroborar la identidad de una entidad (p.ej., una persona, una terminal de computadora, una tarjeta de crédito, etc.

Autorización Únicamente los votantes registrados tienen derecho a emitir votos, y a cada votante debe permitírsele la emisión únicamente de un voto.

Transmisión a otra entidad, o sanción oficial, para hacer o ser algo.

[1] Si un votante puede demostrar que su voto fue emitido de una manera en particular, se abre una ventana a la presión social, familiar o laboral, así como la práctica de compra de votos.

Para desarrollar el tema nodal del trabajo, a dichos objetivos debe agregársele el importante aporte del trabajo de (Halderman 2012, Secc. 1.3): La adición de *accesibilidad* y *disponibilidad* como propiedades relacionadas y secundarias.

Accesibilidad [2] Todos los votantes autorizados tienen la posibilidad de votar; no hay requisitos desmesurados para la participación, ni fuertes asimetrías en la distribución de casillas.

Disponibilidad El sistema electoral puede aceptar todos los votos en el periodo estipulado, y debe producir resultados en un tiempo razonable.

Puede observarse que hay dos tensiones fundamentales entre las propiedades presentadas: Integridad y confidencialidad parecen conllevar objetivos contrapuestos, al igual que autenticación y accesibilidad.

2.2. Seguridad por obscuridad, divulgación controlada y divulgación plena

Teniendo ya definidos los objetivos o propiedades de un sistema seguro en el entorno relevante al tema que abordamos, conviene presentar uno de los argumentos que más reiteradamente se presenta al intentar estudiar fallos como los que presentaremos: La controversia respecto al manejo de la secrecía *del sistema mismo*. Swire 2004 presenta la tensión entre prácticas opuestas:

> La mayoría de los expertos en seguridad en cómputo y redes están familiarizados con el lema que dice que "no hay seguridad a través de la obscuridad." Para quien defiende al software de fuentes abiertas (*Open Source*), revelar los detalles de un sistema tenderá a mejorar la seguridad, notablemente debido a la revisión entre pares. Visto de esta manera, intentar ocultar los detalles de un sistema tenderá a dañar a la seguridad, dado que los atacantes conocerán las vulnerabilidades que tiene, pero los defensores no sabrán dónde corregirlas. En fuerte contraste, un lema famoso de la segunda guerra mundial dice, "los labios sueltos hunden barcos" (*Loose lips sink ships*). Para la mayoría de los expertos en las áreas militares y de inteligencia, la secrecía es una herramienta crítica para mantener la seguridad.

No es casual la comparación con los escenarios de operaciones militares: Antes del surgimiento de la criptografía moderna o incluso de las más rudimentarias computadoras de propósito general, el principio de Kerckhoff enuncia que *un criptosistema debe poderse considerar seguro incluso si todos los detalles respecto al mismo, a excepción de la llave, son de conocimiento público* (Kerckhoff 1883); esto mismo fue enunciado de forma más sucinta en la que se conoce como la *máxima de Shannon* al decir que *el enemigo conoce al sistema* (Shannon 1949, p.662).

Si bien ambos casos se refieren específicamente a la seguridad en sistemas criptográficos, estos planteamientos se han adoptado para los diversos aspectos de la seguridad informática. Las recomendaciones de NIST para asegurar servidores de Internet menciona como el *principio de diseño abierto* (Scarfone, Jansen y Miles 2008):

[2] En inglés, *enfranchisement*. En el plano electoral, en los Estados Unidos es frecuente hablar de su opuesto, *disenfranchisement*, que se traduce como *privación de derechos*; bajo esta óptica, se elige una traducción relacionada con el derecho a *igualdad en el acceso*.

> La seguridad del sistema no debe depender en la secrecía acerca de su implementación o de sus componentes

A pesar de este y otros muchos argumentos en contra de la seguridad por obscuridad, diversas empresas de desarrollo de software, particularmente antes de la masificación de Internet, mantuvieron la política de no divulgar información acerca de los defectos en sus productos, apuntando de este modo a mantener una imagen de fortaleza. Esto, claro, típicamente equivale a sostener un engaño.

Entre los años 2000 y 2010 se presentó un interesante debate en la industria y la academia respecto al correcto manejo de la divulgación de fallos; si bien pocos argumentarían hoy en día a favor de una absoluta *no divulgación*, se presentó un interesante debate con importantes opiniones a favor de la *divulgación coordinada* o *divulgación responsable* (Culp 2001) y la *divulgación plena* (Schneier 2007). Hoy en día, si acaso, el debate se centra más acerca de los *parámetros* que toma la divulgación coordinada (Frei y col. 2010), y la práctica se toma ya como un estándar en el campo de la seguridad informática (Christey y Wysopal 2002; Arora, Telang y Xu 2008).

Este tema se trae al presente trabajo dado que uno de los reductos en que sigue imperando la política de la no divulgación es, precisamente, en temas relativos al voto electrónico. Prácticamente la totalidad tanto de las empresas como las entidades gubernamentales dedicadas al desarrollo de equipos y sistemas para el voto electrónico tienen una estricta política de no divulgación, y casos como el relatado por Prasad y col. 2010 o el acoso judicial posterior a la divulgación de información del que fue objeto Smaldone 2015 (casos que serán ambos presentados en el Capítulo 4) refieren a prácticas que podrían creerse desterradas.

2.3. Modalidades de emisión del voto

Habiendo cubierto estos puntos necesarios para el análisis desde la seguridad de la información, corresponde enmarcar el objeto directo de estudio del presente trabajo: Las principales modalidades que a lo largo de la historia de la humanidad se han utilizado para la emisión de los votos. Se presenta a continuación una breve reseña histórica de las principales modalidades que han sido utilizadas; pueden encontrarse numerosos trabajos pormenorizando las ventajas y desventajas relativas de cada uno de ellos (Douglas W. Jones 2003; R. Saltman 2006; Chief Electoral Officer of Canada 2007). Puede apreciarse que, muy desde el principio y siglos antes aún de los sistemas automatizados, ya se perseguían los objetivos de la seguridad de la información.

Las modalidades de votación pueden clasificarse por el principal mecanismo empleado para la emisión del voto, como lo presenta la figura 2.1. El tipo de sistema empleado resulta particularmente importante para comprender el funcionamiento y la madurez política de una sociedad, dado que ha observado repetidamente que el sistema electoral puede funcionar como barómetro para definir la vida política (y, de cierto modo, la salud interna) de una sociedad (Elizalde 1977).

Para el presente trabajo el análisis se centra en la *emisión* del voto. Hay muchas otras formas de clasificar el funcionamiento del sistema electoral de un país, región u organización, sea respecto a cómo se reparten las proporciones de votos recibidos, a si permiten o no un voto por diferentes listas o partidos en distintas subelecciones, o incluso si están centrados en la *persona* como candidato al cargo o en la *lista partidaria* como representante de una ideología (Nohlen 1998); el enfoque perseguido se centra en la emisión, almacenamiento y totalización de votos. Cabe mencionar que la lista presentada a continuación no es exhaustiva ni detallada; hay numerosas posibilidades de refinar cada una de las modalidades descritas. La principal razón para realizar el presente listado es para posteriormente (véase la Sección 4.1.1) detallar el ámbito al que se limita el estudio realizado.

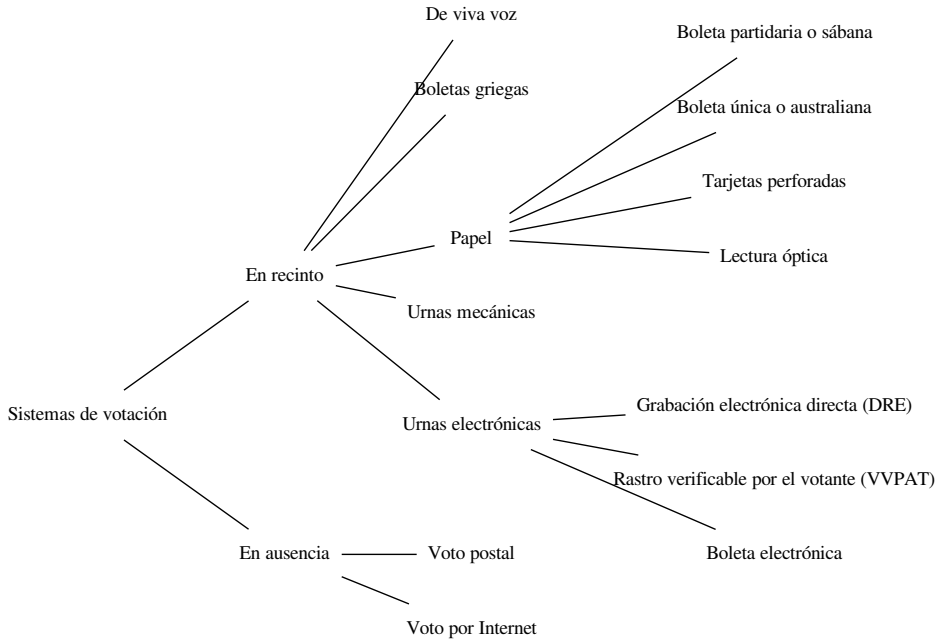


Figura 2.1: Principales esquemas de votación empleadas a lo largo de la historia

Viva voz El mecanismo más natural de emisión de votos es *a viva voz*; cada participante de una decisión proclama en voz alta y públicamente su preferencia. De este modo, todos los interesdos pueden llevar la contabilidad de los sufragios, permitiendo garantizar la integridad de los resultados.

En la mayor parte de los países democráticos del siglo XIX, el votante acudía al recinto electoral, donde indicaba *de viva voz* a las autoridades electorales su preferencia. Es pertinente hacer referencia en este punto a la pintura *la elección en el condado* (Bingham 1846), en que el autor ilustra muchos de los vicios observados en la mecánica electoral prevaleciente en su tiempo.

Las votaciones a viva voz comprometen completamente la propiedad de confidencialidad descrita en la sección anterior (no puede existir el secreto electoral); si bien esta modalidad era común en diversos sistemas electorales nacionales del siglo XIX, ya desde principios del siglo XX se registra su desaparición en prácticamente todos los ejercicios electorales.

Boletas griegas El primer registro de un sistema de votación que contempla la *confidencialidad* es de la Grecia clásica: Los votantes depositaban pedazos de arcilla con el sentido de su voto escrito en una urna. Esta práctica se encuentra de nuevo en las sociedades secretas del Renacimiento, como la masonería, en que un voto consiste de una *pequeña bola* (en italiano, *ballota*, raíz de donde derivan tanto la palabra *boleta* en español como *ballot* en inglés).

Al depositar las boletas en una urna cerrada y opaca, en presencia de los pares votantes, se asegura la emisión del voto por parte de todos los participantes. Requiere que la *ceremonia electoral* sea en un momento determinado, no a lo largo de un día entero, y limita el tamaño práctico de una estación de emisión de votos.

Este esquema, fuera de entornos rituales como el de la masonería, fue reemplazado por los dos que se exponen a continuación (*boleta partidaria o sábana* y *boleta única o australiana*), en principal medida por razones de practicidad.

Boleta partidaria o sábana En un sistema basado en partidos, se denomina de esta forma el sistema electoral si es a) *plurinominal* (presenta a más de un candidato), *grande* (presenta listas con un mínimo de diez candidatos), y *cerrada o bloqueada* (la lista debe integrarse por candidatos del mismo partido, en el orden determinado por el partido) (Tula 2006). El votante emite su voto seleccionando una boleta de entre las provistas por los partidos, e introduciéndolo en un sobre (que asegura la confidencialidad del voto), mismo que es depositado en la urna.

En algunos sistemas electorales, se permite *cortar boleta* — El votante puede introducir al sobre *fragmentos* de la boleta de diferentes partidos, aunque siempre conservando la unidad por cargo (esto es, no cortar dentro de la lista de contendientes para un mismo cargo, sino que entre dos cargos distintos: Votar por el presidente de un partido y por los diputados de otro).

Este sistema es el dominante en Europa; en América Latina, es el sistema históricamente utilizado en Argentina, aunque ha sido ya abandonado por muchas de sus provincias (Tula 2006).

Boleta única o australiana Esta modalidad se presenta en los sistemas donde la boleta para cada una de las elecciones concurrentes contiene a la lista de todos los partidos o candidatos que compiten por el puesto. Puede contener un espacio para el voto en blanco o para inscribir a un candidato no partidario. Las boletas son diseñadas e impresas por la autoridad electoral, y su distribución es restringida al recinto electoral.

Esta forma de votación se presentó por primera vez en Australia, en 1856, y es hoy en día dominante en América Latina. Es el sistema empleado en México.[3]

Urnas mecánicas Uno de los procesos más tediosos de la jornada electoral es el conteo de votos. Intentar automatizar este proceso no es novedad — Ya en 1892, en Lockport, Estado de Nueva York, se votó utilizando medios mecánicos (Bird 2004): En vez de emplear una urna, el votante indica el sentido de su voto cambiando la posición de una serie de palancas, de forma que al marcar la palanca maestra, los totales (mantenidos dentro del engranaje de la máquina) se actualicen. El resultado de la votación se puede, por tanto, obtener de forma instantánea al declarar finalizada la jornada electoral: Basta abrir la máquina y ver los totales.

Desde muy temprano, las dudas respecto a la confiabilidad de estas máquinas se han hecho patentes. Citando al Juez Horatio Rogers en 1898 (traducción propia), *un votante en esta máquina no tiene conocimiento mediante sus sentidos de que ha logrado un resultado... Lo más que pude decir es que, si la máquina funcionó como debía, ha votado* (Douglas W Jones 2010).

Las máquinas de votación se popularizaron en los Estados Unidos, y hacia mediados del siglo XX, la mayor parte del país votaba con urnas mecánicas. Estas son, sin embargo, susceptibles a desgaste mecánico que puede llevar a la pérdida de votos (por ejemplo, un engrane desgastado puede no arrastrar confiablemente su totalización) y su mantenimiento es costoso; son la primera tecnología con amplia base instalada en que se presenta la *desmaterialización del voto* (Busaniche y Heinz 2009). Hoy en

[3] En el caso particular de México, una jornada electoral consta típicamente de múltiples *elecciones paralelas*, razón por la cual se reparten al votante múltiples boletas electorales, mismas que siguen una codificación cromática para ser depositadas en distintas urnas. Cada elección, pues, es realizada mediante una boleta única.

día y a raíz de la ley HAVA de 2002 (Janicki 2003) que asigna expresamente fondos federales para su reemplazo, su uso se ha abandonado casi por completo.

Lectura óptica Con el avance de la electrónica apareció el primer sistema que, sin caer en la desmaterialización del voto (cada boleta sigue siendo una entidad tangible y con permanencia en el tiempo), permite un conteo y totalización de los votos ágil y casi instantáneo: La lectura óptica de boletas con un formato preestablecido. Esta tecnología, hoy en día ampliamente utilizada eminentemente para los exámenes estandarizados, fue utilizada por primera vez en el condado de Kern (Bakersfield), California, en 1962.

Tarjetas perforadas Una tecnología análoga a la de lectura óptica es la de tarjetas perforadas. Si bien éstas se inventaron ya a principios del siglo XVIII para controlar el funcionamiento de telares, y se emplearon por primera vez para la tabulación y totalización de datos en el censo de 1890 en los Estados Unidos, fue apenas en 1964 que se utilizaron por primera vez para la emisión y totalización del voto en el estado de Georgia, Estados Unidos, en 1964.

Las tarjetas perforadas se popularizaron en los Estados Unidos, y tuvieron amplia adopción en los Estados Unidos. Sin embargo, tanto por reportes de vulnerabilidad de los sistemas totalizadores como por las deficiencias mecánicas de la cartulina perforada que llevan a falsas lecturas (R. G. Saltman 1988), y particularmente la traumática experiencia del recuento en Florida de la elección del año 2000 (Commission on Federal Election Reform 2005) han llevado a que al día de hoy su uso se haya casi abandonado.

Grabación electrónica directa (DRE) La primera generación de equipos de voto electrónico claramente calificables como tales son los de grabación electrónica directa (DRE). Estas pueden verse como análogas a las urnas mecánicas, pero con la ventaja de la reconfigurabilidad y flexibilidad que brinda el implementarse sobre sistemas de cómputo: Los votos recibidos se van acumulando en memoria en el transcurso de la jornada electoral, y entrega el resumen al indicar las autoridades electorales que deben totalizar.

La crítica que se hace más frecuentemente a los sistemas DRE es que lleva nuevamente a una *desmaterialización del voto*: La *verdad electoral* es el estado de la memoria de la urna electrónica, y no existe la posibilidad de realizar un recuento, pues los votos mismos no están sustentados en ningún documento físico; se presentará la respuesta a esta crítica en el siguiente inciso (VVPAT).

Las primeras implementaciones de DRE datan de principios de los 1980, pero tuvieron adopción limitada; Brasil, la India y Venezuela son los principales ejemplos de la adopción a escala nacional de sistemas electorales basados en DRE y que los siguen utilizando al día de hoy; Holanda se cuenta también entre los primeros países en emplear DRE, pero lo abandonó en 2006 tras profundas demostraciones públicas de inseguridad (Jacobs y Pieters 2009).

Rastro Verificable por el Votante (VVPAT) Esta modalidad nace como respuesta a la crítica anteriormente mencionada a los equipos *DRE*: Además de registrar los votos en la memoria de la urna electrónica, los equipos VVPAT imprimen un comprobante físico en papel (típicamente denominado *testigo*), para que sirva como evidencia en caso de requerirse un recuento. Curiosamente, la tecnología VVPAT no nació con el voto electrónico, sino con el voto mecánico hace más de un siglo (Gray 1899), pero no tuvo mayor adopción sino hasta el presente siglo, a partir del trabajo de Mercuri 2001.

La manera en que opera VVPAT varía: En algunos sistemas, el comprobante es emitido tras una ventanilla de la urna electrónica, permitiendo al votante confirmar la información impresa pero no manipular al *testigo* directamente; en otros, el *testigo* es entregado al votante, quien lo deposita en una urna.

Boleta electrónica La boleta electrónica lleva un paso más allá lo planteado por VVPAT: La urna electrónica es el equipo empleado para emitir el voto, y no guarda registro de cada uno de ellos. Los votos son almacenados electrónicamente en la boleta e impresos sobre la misma; la totalización se efectúa pasando las boletas sobre un equipo lector, y las mismas boletas pueden ser empleadas como *testigos*.

La boleta electrónica fue creada directamente como respuesta a la legislación argentina que establece que la votación debe efectuarse mediante equipos *sin memoria ni capacidad de almacenar el registro de los votos* (Ciudad Autónoma de Buenos Aires 2014, Anexo I, artículo 24, párrafo p).

Una vez finalizada la etapa de emisión de votos, las boletas electrónicas son leídas por equipos acorde, realizando la totalización de forma electrónica; los *testigos* legibles por humano son, al igual que en VVPAT, para ser empleados únicamente en caso de contingencia.

Voto postal Todas las modalidades cubiertas hasta este punto requieren que los votantes se trasladen al recinto electoral para emitir su sufragio. Hay muchas situaciones que pueden dificultar o imposibilitar el desplazamiento del votante al recinto electoral, razones que pueden cubrir desde enfermedades incapacitantes hasta el no estar en la jurisdicción en la fecha de votación (ya sea de forma permanente, por ejemplo, en el caso de un residente en el extranjero, o temporalmente por un viaje).

Australia fue también pionero en el voto postal: La primer aplicación de esta modalidad de votación fue en el Estado de Australia Occidental, en 1877 (Sawer, Abjorensen y Larkin 2009, pág. 107). Hoy en día, este modelo ha sido empleado por países de todo el mundo, incluyendo México, desde 2005 (Peschard 2007, pág. 148); en los Estados de Colorado, Oregon y Washington de los Estados Unidos las elecciones se celebran exclusivamente por vía postal.

Voto por Internet El voto por Internet se presenta como la progresión natural del voto postal, con la diferencia fundamental de que, en vez de enviarse en sobre cerrado por correo, el voto se emite por Internet. De la totalidad de modalidades mencionadas en este apartado, esta es la que menos exposición al público a tenido a la fecha; el caso más conocido de implementación de voto por Internet a nivel nacional es el de Estonia, país que implementó una *tarjeta inteligente* de identificación a nivel nacional que es utilizada (mediante hardware lector ampliamente disponible) para la autenticación (Springall y col. 2014). En la Sección 4.3.19 se hace referencia al análisis externo realizado a esta implementación.

No todas las modalidades cubiertas son cubiertas por este trabajo; la Sección 4.1.1 presenta la delimitación de su ámbito de estudio.

2.4. Taxonomías de vulnerabilidades

Dado que buscamos obtener características comunes a un conjunto de casos de fallo en la aplicación del voto electrónico, a continuación desarrollamos una vista general de las *taxonomías de vulnerabilidades* sobre las cuales se desarrolla el trabajo.

En las últimas cuatro décadas se han desarrollado una gran cantidad de taxonomías para la clasificación de fallos informáticos. Algunas buscan especializarse en visiones particulares del espacio de problema, otras intentan ser tan globales y genéricas como sea posible.

Dado el avance de los usos de la tecnología, hay una innegable tendencia a una rápida obsolescencia, ya que en todo momento, los sistemas de cómputo se han desarrollado en consonancia con los avances y particularidades tecnológicas de su momento en el tiempo. Además, periódicamente se descubren nuevas categorías de vulnerabilidad, que pueden obligar a re-evaluar a los sistemas para determinar si dicha vulnerabilidad se presenta en ellos.

Ante la cantidad de taxonomías de vulnerabilidades existente, con el paso del tiempo se han publicado *comparaciones entre taxonomías*. Para el desarrollo del presente trabajo, se ha hecho referencia particularmente a Polepeddi 2005; Igure y Williams 2008 Hui y col. 2010; Tripathi y Singh 2010; Joshi, Singh y Tarey 2015.

A partir de dicha revisión, se seleccionaron las siguientes taxonomías como punto de partida para la elaboración de este trabajo, mismas que serán abordadas según lo indica el Cuadro 2.1. Para cada una de las taxonomías, por simplicidad de referencia interna, se indican únicamente las siglas con las cuales se hace referencia a ella en el transcurso de la presente obra.

Cuadro 2.1: Taxonomías desarrolladas empleadas para el desarrollo de la investigación

Sigla	Nombre	Referencia	Representación en Sección	Evaluación en Sección
7RP	*Siete reinos perniciosos*	Tsipenyuk, Chess y McGraw 2006	4.2.1	5.2
ROdC	*Riesgos Operacionales de Ciberseguridad*	Cebula, Popeck y Young 2014	4.2.2	5.3
AASVU	*Análisis de Amenazas en Sistemas de Votación UOCAVA*	Regenscheid y Hastings 2008	4.2.3	5.4

A continuación se presentan las características principales de cada una de ellas; cabe mencionar que las propuestas de cada una de las taxonomías describen el dominio que cubren, pero no presentan una *representación* apta para cada uso. Dado que este trabajo persigue facilidad en la comparación de resultados, se juzgó fundamental diseñar una representación acorde para cada una de ellas, misma que será abordada en la Sección 4.2.

2.4.1. 7RP: Siete Reinos Perniciosos

La primera taxonomía empleada en el presente trabajo fue presentada, primero a *vuelo de ave* en Tsipenyuk, Chess y McGraw 2005, y a mayor profundidad en Tsipenyuk, Chess y McGraw 2006, busca catalogar las principales malas prácticas de programación que frecuentemente llevan a errores, algunos de los cuales pueden convertirse en fallos de seguridad. Uno de los criterios para el desarrollo de esta taxonomía es la simplicidad en su aplicación; citando del primero de dichos textos (traducción propia),

> Hemos visto muchas taxonomías orientadas a seguridad a lo largo de los años, y todas comparten una desafortunada característica — Son demasiado complejas. La gente es buena para dar

> seguimiento a siete cosas simultáneas (más o menos dos), así que utilizamos este número como una restricción dura, intentando mantener al número de *reinos* en siete (mas uno).

Los siete *reinos* en que según esta taxonomía se catalogan los fallos de seguridad son:

1. Validación y representación de entradas
2. Abuso de APIs
3. Características de seguridad
4. Tiempo y estado
5. Errores
6. Calidad del código
7. Encapsulamiento

Menciona el texto citado un *octavo* reino, justificado de la siguiente manera por los autores (traducción propia):

> *Ambiente:*
>
> Esta sección incluye todo lo que está fuera del código fuente, pero es de todos modos crítico a la seguridad del producto que se está creando. Dado que la problemática cubierta por este reino no está directamente relacionada con el código fuente, la separamos de los otros reinos.

Este octavo reino se mantiene como externo y relacionado al no derivarse directamente del desarrollo de software (sino que de su despliegue). Cabe referirse, sin embargo, a Bishop 2002: ¿Qué tan adecuado puede resultar clasificar a una vulnerabilidad como *error en el ambiente* y no *en el código*? ¿No es acaso un error en el código no verificar que el ambiente sea correcto, y por tanto, un error en el ambiente es una manifestación alternativa de un error en el código?

Por último, partiendo de la gran cantidad de taxonomías preexistentes, esta taxonomía presenta un mapeo entre los *reinos* que define, los *19 pecados mortales de la seguridad en software* (M. Howard, LeBlanc y Viega 2005) y los *Top Ten de OWASP* (OWASP 2004). Los autores indican que la principal ventaja de 7RP por sobre éstos es su mayor simplicidad y un nivel de abstracción más homogéneo; la Figura 2.2 (traducción directa de aquella publicada en Tsipenyuk, Chess y McGraw 2005) presenta un mapeo entre estas taxonomías.

Cuadro 2.2: Mapeo de los *reinos* a *19 pecados*, *OWASP* (Tsipenyuk, Chess y McGraw 2005)

7RP	**19 pecados**	**OWASP Top Ten**
Validación y representación de entradas	Desbordamientos de buffer, inyección de comandos, *cross-site Scripting* (XSS), problemas en cadenas de formato, errores de rangos de enteros, inyección de SQL	Desbordamientos de buffer, fallas de Cross-site scripting (XSS), fallas de inyección, entradas no validadas
Abuso de APIs	Confiar en la información de las direcciones de red	

Continúa en la siguiente página

Continúa de la página anterior

7RP	19 pecados	OWASP Top Ten
Características de seguridad	Errores al proteger tráfico de red, errores en el almacenamiento y protección de datos, errores en el uso de números aleatorios criptográficamente fuertes, acceso inadecuado a archivos, uso inadecuado de SQL, uso de sistemas débiles basados en contraseña, intercambio de llaves sin autenticación	Control de acceso roto, almacenamiento inseguro
Tiempo y estado	Condiciones de carrera en señales, uso de URLs "mágicas" y formas ocultas	Administración de autenticación y sesión rota
Errores	Manejo inadecuado de errores	Manejo inadecuado de errores
Calidad del código	Usabilidad pobre	Denegación de servicio
Encapsulamiento	Filtración de información	
Ambiente		Administración insegura de la configuración

La representación de *7RP* empleada para este trabajo se detalla en la Sección 4.2.1.

2.4.2. ROdC: Riesgos Operacionales de Ciberseguridad

La segunda taxonomía abordada es presentada por Cebula, Popeck y Young 2014 como parte del trabajo del CERT CMU[4] bajo el título «Una taxonomía de riesgos operacionales de ciberseguridad» (*A Taxonomy of Operational Cyber Security Risks*). Esta taxonomía está orientada a organizar las *fuentes de riesgo operacional* jerárquicamente, en un árbol (véase la Figura 2.2) que inicia a partir de cuatro grandes áreas:

1. Acciones de personas
2. Fallas de sistemas y tecnología
3. Procesos internos fallidos
4. Procesos externos

Al desarrollar esta taxonomía, se hace referencia a cada una de sus *categorías* de último nivel (las *hojas* del árbol) por su ruta numérica; por ejemplo, para referirse a *inacción por falta de conocimiento* se indica *1.3.2*, donde *1* denota *Acciones de personas*, *1.3* apunta a *Inacción*, y *1.3.2* representa *Conocimiento*.

Esta taxonomía busca ayudar a sus usuarios a dar los primeros pasos al determinar el nivel global de seguridad relativo a un sistema, particularmente enfocado a la *administración de riesgos*, ayudando a la comprensión de las condiciones y consecuencias relacionadas con el estado general del sistema.

Al presentarse esta taxonomía, el documento en que está sustentada busca armonizar con las mejores prácticas en el tema; hace referencia explícita a documentos tanto de aplicación específica a las necesidades

[4] *Equipo de Respuesta a Emergencias de Cómputo*, o CERT por sus siglas en inglés. El primer equipo con este nombre se creó en el Instituto de Ingeniería en Software de la Universidad Carnegie Mellon; al día de hoy, el Centro de Coordinación de equipos CERT opera en dicha universidad.

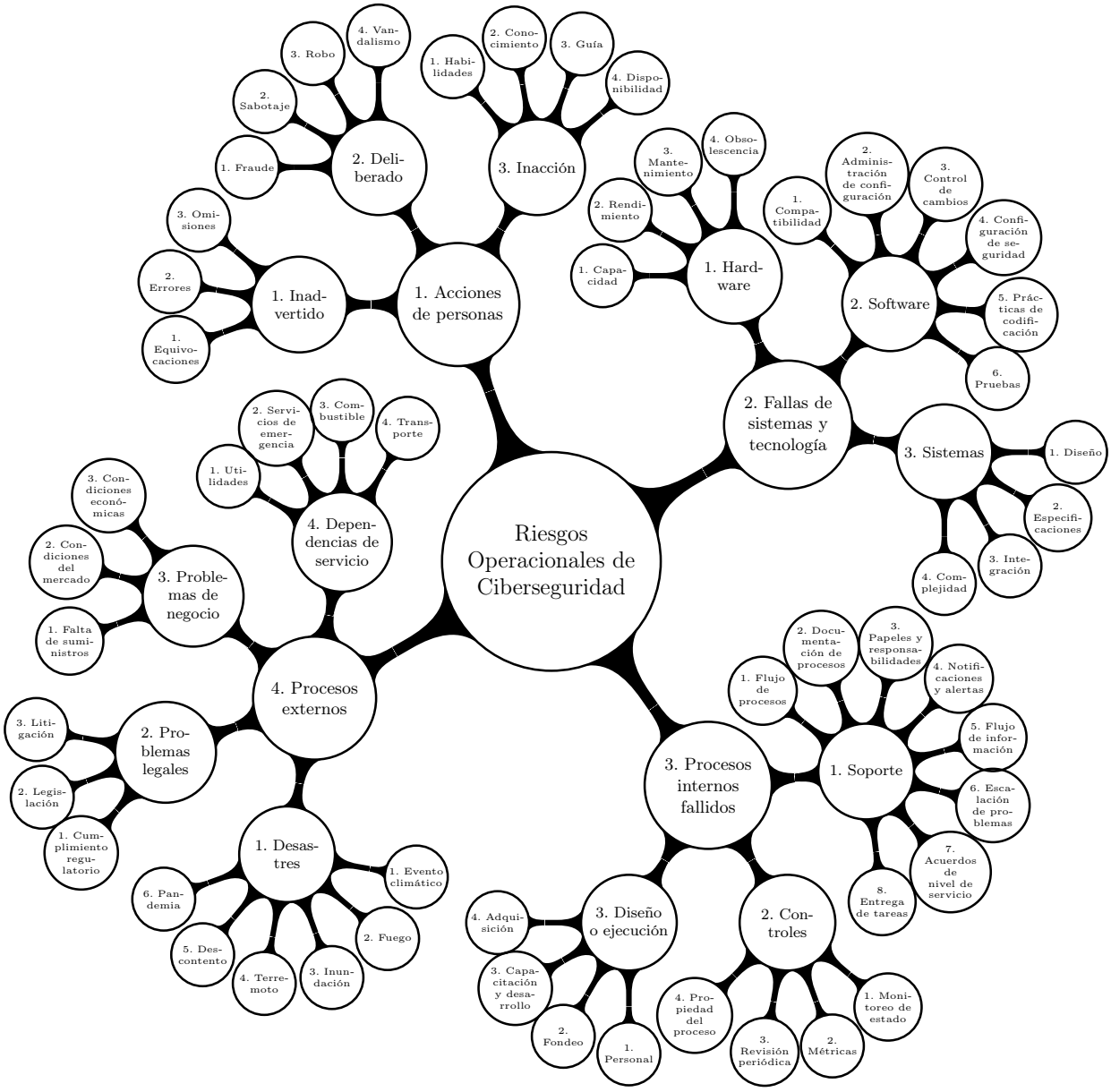


Figura 2.2: Árbol de la taxonomía ROdC

del gobierno de los Estados Unidos, como FISMA (107th Congress of the United States of America 2002) y NIST SP 800-53 (JTF-TI 2013; Dempsey, Witte y Rike 2014), como a la metodología OCTAVE para la evaluación comprehensiva de riesgos de seguridad (Caralli y col. 2007).

En el caso de NIST SP 800-53, el Apéndice A del trabajo citado presenta un mapeo de las diversas categorías de NIST hacia las clases correspondientes de RODC — A modo de ejemplo, NIST-SP 800-53 define la clase *AC* (Control de Acceso), dentro de la cual *AC-19* se refiere al *Control de acceso para dispositivos móviles*. Las categorías correspondientes a RODC para una falla de este tipo son 1.1 (personal inadvertido), 1.2 (personal deliberado), 2.1 (hardware), 2.2 (software), 3.1 (diseño o ejecución de procesos) y 4.2 (problemas legales).

La Sección 4.2.2 muestra la estrategia encontrada en el desarrollo del presente proyecto para la representación de la información resultante de esta taxonomía.

2.4.3. AASVU: Análisis de Amenazas en Sistemas de Votación UOCAVA

En tercer lugar, se presenta la aplicación del trabajo presentado por Regenscheid y Hastings 2008. Si bien éste no se presenta originalmente como una taxonomía, sino como un reporte de amenazas que presentan las diferentes formas de votación a distancia,[5] buscando llevar a lineamientos de mejores prácticas.

Este reporte parte de la presentación de los métodos de votación a distancia empleados por los Estados Unidos para su población registrada como *en ausencia*, esto es:

1. Vía telefónica
2. Fax
3. Correo electrónico
4. Votación por Web

El proceso de votación definido por UOCAVA consta de cinco pasos, pero el reporte las agrupa en únicamente tres dado lo similares que resultan algunos de los pasos:

1. Registro de votante y solicitud de boletas
2. Distribución de boletas
3. Retorno de boleta con voto

Regenscheid y Hastings 2008 presentan su metodología de análisis de riesgo desarrollada sobre dichos vectores, mismos que se aplican en el presente trabajo, basada en los puntos que presenta la Figura 2.3.

Al igual que en el caso anterior, AASVU también se presenta como únicamente un primer paso en la tarea de administración del riesgo en el entorno UOCAVA; el análisis que presentan está basado en NIST SP 800-30 (Stoneburner, Goguen y Feringa 2002), y refiere a los controles presentados en NIST-SP 800-53 (JTF-TI 2013; Dempsey, Witte y Rike 2014) para su atención.

La forma de representar el análisis de cada uno de los casos abordados sobre esta taxonomía se aborda en la Sección 4.2.3.

[5] Las siglas UOCAVA se refieren a *Uniformed and Overseas Citizens Absentee Voting Act* (Ley para la Votación en Ausencia de Ciudadanos Uniformados y en el Extranjero).

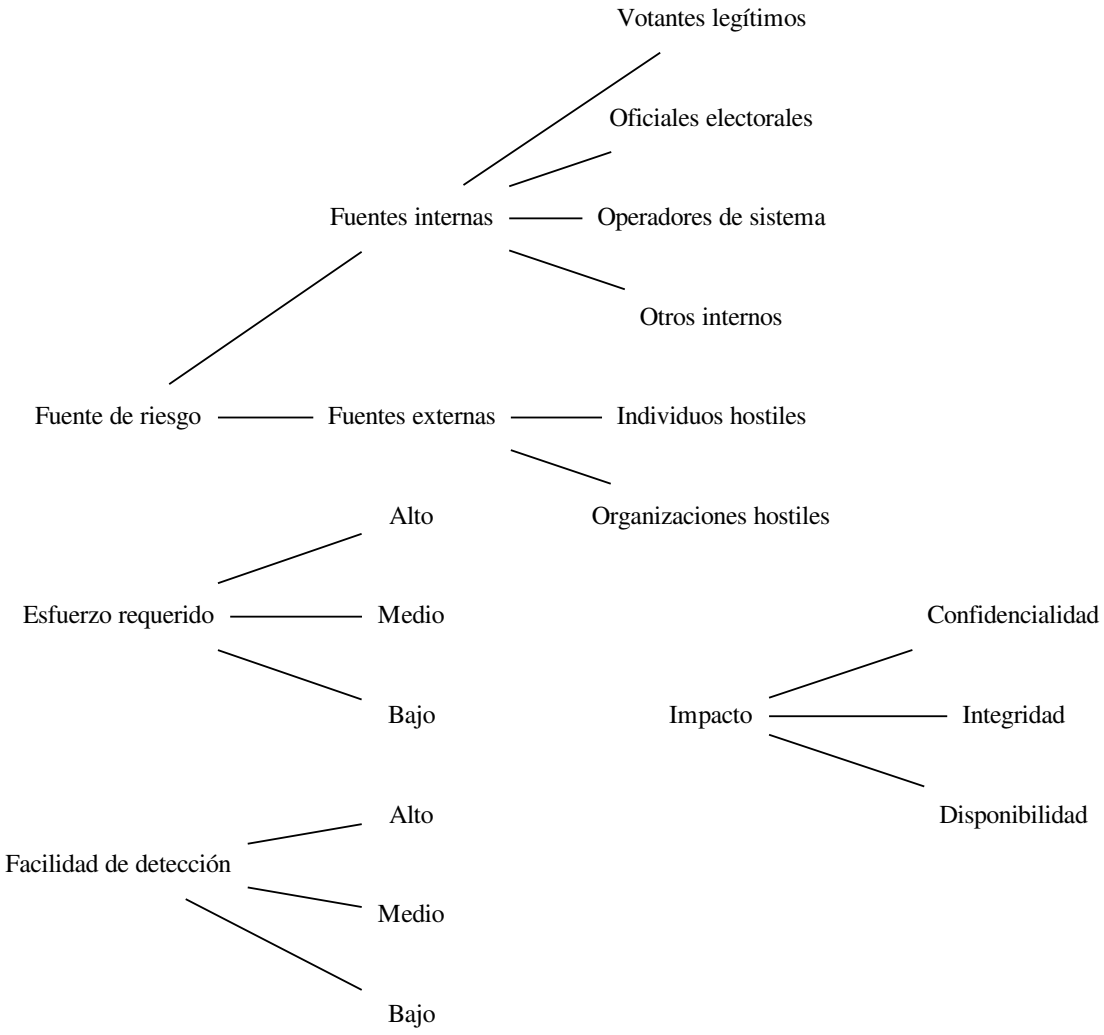


Figura 2.3: Puntos del análisis de riesgos AASVU

2.5. Modelos de madurez

Frecuentemente, las taxonomías descritas en la sección anterior sirven como base para el desarrollo de *modelos de madurez*.

Los *modelos de madurez* son lineamientos concebidos para ayudar a cuantificar de forma simple, metódica y unidimensional el avance sobre un proceso evolutivo de mejora, comprendiendo *madurez* como *estar completo, perfecto o listo* (Mettler y Rohner 2009); son útiles para guiar a una organización en el desarrollo de procesos que lleven a un estado de madurez en el área para la cual se desarrolló el modelo. (G. B. White 2007) Citando a Saleh 2011 (traducción propia):

> El concepto de los modelos de madurez está siendo aplicado cada vez más dentro del campo de los Sistemas de Información como un enfoque para el desarrollo organizacional, o como un medio para la evaluación organizacional. Cualquier marco sistemático para la realización de mediciones y mejoras en el rendimiento puede ser considerado un modelo, y si cuenta con procesos de mejora continua puede ser considerado un modelo de madurez. Ser maduro implica el que un sistema esté completo. Generalmente, en la literatura constitutiva del campo, la madurez implica perfección, o un sistema explícitamente definido, administrado, medido y controlado. También es un progreso en la demostración de una capacidad específica, o en el logro de un objetivo a partir de un estado inicial.

En este campo se presenta un panorama similar al mencionado en la sección 2.4: En los primeros quince años transcurridos desde la publicación del Modelo de Madurez en Capacidades (CMM) se publicaron 135 distintos modelos de madurez (Mettler y Rohner 2009); el simple hecho de seleccionar *cuál* modelo de madurez perseguir requiere una comprensión del campo, así como tener muy claro lo que se busca alcanzar mediante su aplicación.

A continuación, se presentan algunos de los principales modelos de madurez; en la Sección 5.5 se presentarán las conclusiones alcanzadas acerca de su aplicabilidad al presente trabajo.

BSIMM El *Modelo de Construcción de Seguridad mediante la Madurez* (*Building Security in Maturity Model*) (McGraw, Migues y West 2015) está orientado a la madurez de las actividades relacionadas con el desarrollo de software, derivado de la observación repetida de las mejores prácticas en un grupo de empresas de escala global.

ISMM Saleh 2011 hace una revisión sobre el desarrollo y los objetivos que persiguen los distintos modelos de madurez, y los aplica al campo de la seguridad informática para crear el *Modelo de Madurez de Seguridad de la Información* (Information Security Maturity Model), buscando medir la madurez en seguridad de una organización mediante cuatro *indicadores núcleo* y un modelo simple de aplicar, basado en un cuestionario con puntos a calificar de forma inambigua, sea de forma binaria o en escala discreta.

CCSMM El *Modelo de Madurez de Ciber Seguridad Comunitaria* (Community Cyber Security Model) (G. B. White 2007; Sjelin y G. White 2017) busca medir la seguridad ya no de una empresa o entidad de gobierno por separado, sino de una *comunidad* (siguiendo el eje de agregación empresa → comunidad → estado → nación); para que la seguridad agregada de las comunidades alcance mayores niveles de madurez, su planteamiento hace mucho énfasis en la necesidad de *compartir información* entre las distintas empresas o entidades; citando de G. B. White 2007 (traducción propia):

> La comunicación acerca de riesgos y ataques en sistemas del gobierno local y de infraestructura crítica es difícil por muchos factores. En primer lugar, no existe una predisposición mental para compartir. Las organizaciones rara vez quieren alertar a terceros respecto a fallas en su seguridad. (. . .) Los ataques frecuentemente no son eventos aislados: Lo que una organización experimenta probablemente también sea experimentado por otras. Si una entidad descubre el ataque, comunicar esta información a otros puede ayudarlos a determinar si también les está afectando.

ISCMM El *Modelo de Madurez de Competencia en Seguridad de la Información* (Information Security Competence Maturity Model) (Thomson y Solms 2006) no se presenta, a diferencia de los anteriores, como un modelo de madurez plenamente desarrollado, sino que como un trabajo en proceso (el artículo citado se titula, *Hacia un Modelo de Madurez de Competencia en Seguridad de la Información*), pero toca aspectos importantes a considerar, particularmente la madurez en las costumbres relacionadas con la seguridad de la información entre los empleados de una empresa. Dado que para el presente trabajo es de gran importancia, como se expondrá, el papel de las personas involucradas en lograr un nivel aceptable de seguridad, resulta muy relevante incluir este modelo.

Capítulo 3

Estado del arte

3.1. Comparativas entre taxonomías de seguridad informática

Hay muchos factores detrás de la decisión de basar este estudio sobre taxonomías orientadas a la seguridad informática, pero entre todos ellos, resuena claramente la hipótesis central que menciona en su tesis doctoral Lough 2001 (en traducción propia):

> Un número finito de ataques y vulnerabilidades computacionales puede ser clasificado dentro de una taxonomía, y dicha taxonomía, junto con metodologías aplicables, puede ser utilizada para predecir futuros ataques.

Landwehr y col. 1994 explica claramente la importancia y el papel que juegan las taxonomías en la comprensión del mundo desde el ángulo que se decida estudiar:

> Una taxonomía no es simplemente una estructura neutral para categorizar especímenes. Implícitamente da cuerpo a una teoría del universo desde el cual dichos especímenes son seleccionados. Define qué datos se considerarán, y cómo se deben distinguir especímenes con mayor o menor similitud. Al crear una taxonomía de fallos de seguridad en programas de cómputo, estamos creando una teoría de dichos fallos, y si buscamos respuestas a preguntas particulares de una colección de instancias de fallo, debemos organizar la taxonomía de forma acorde.

Lough inicia su trabajo haciendo una revisión histórica de la seguridad informática, e integra los trabajos de Amoroso 1994, Lindqvist y Jonsson 1997, Krsul 1998 y J. D. Howard 1997, presentando las siguientes propiedades que deben formar parte de una clasificación para conformarse como una verdadera taxonomía. Indica que, idealmente, una taxonomía aplicable a la seguridad informática debe ser:

- *Aceptada* por la comunidad general en que se aplica
- *Apropiada* para un conjunto de suposiciones básicas
- *Basada en el código, ambiente u otros detalles técnicos*, no en causas sociales de una vulnerabilidad
- *Comprensible* tanto para expertos en seguridad como para gente menos familiarizada con el campo
- *Completa*, de forma que todo ataque pueda caber en algún punto de su estructura

- Cada característica puede obtenerse de forma *determinista*, debe haber una manera clara de "extraer" su presencia
- *Exhaustiva*, cubriendo todas las posibles categorías (aunque sea mediante un campo "otros")
- Deben diferenciar *amenazas internas de externas*, para poder plantear un perímetro de seguridad
- Cada categoría debe ser *mutuamente excluyente* respecto a las demás, no debe haber áreas comunes
- Debe haber *objetividad* al determinar la clasificación; las características deben ser identificables desde el objeto conocido, no gracias al conocimiento del sujeto conocedor.
- Las respuestas que conforman a una taxonomía deben ser *primitivas* (sí/no), para facilitar la repetibilidad de la clasificación por un tercero.
- *Fallos similares deben clasificarse de forma similar*, la taxonomía debe representar la cercanía en las características de los fallos.
- Ser *específica* al dominio en que se aplica.
- *Cumplir con la terminología ya establecida* en el campo de la seguridad informática.
- Debe presentar *términos bien definidos*.
- Los términos deben ser *inambiguos*.
- Debe ser *útil*.

Dichos puntos son presentados como un *estándar dorado*; muchas taxonomías no cumplen con todos los criterios citados, pero es deseable que cumplan con la mayor cantidad de ellos posible.

El diseño de una taxonomía no es una tarea sencilla, y Krsul 1998 da amplio fundamento de ello, haciendo una crítica de taxonomías de errores, explotaciones y ataques relativos a la seguridad informática. Parte desde la definición misma y los más de dos milenios de historia de las taxonomías en general, y presenta una gran cantidad de taxonomías desarrolladas específicamente para los distintos aspectos del campo de la seguridad en cómputo desde 1975 y en un periodo de más de 20 años. Si bien la profundidad del estudio que realiza es muy amplia, el estudio que realiza y el enfoque en amplitud que lleva hace que las taxonomías cubiertas resulten demasiado antiguas.

La tesis de Krsul fue publicada en 1998, y dado que una gran parte de las taxonomías que cubre tenían ya más de diez años para ese momento, de este trabajo fue posible obtener importantes definiciones y acotaciones metodológicas, pero ninguna de las taxonomías que aborda resultaron relevantes al estudio presente.

Al hacer comparaciones de taxonomías a profundidad, Bishop y Bailey 1996 presenta la dificultad de clasificar de forma clara e inambigua un par de casos ejemplo de fallo de seguridad mediante tres taxonomías clásicas y bien conocidas, dos de ellas con dos décadas y una relativamente joven al momento del estudio realizado. Muestra cómo una determinada vulnerabilidad puede ser clasificada distintas maneras, dependiendo de cuál objeto (de entre el sistema operativo, un programa específico, y un conjunto de archivos que dicho programa manipula) es tomado como objeto primario de estudio y cuáles como secundarios. El artículo concluye en hacer el llamado a aplicar criterios de unicidad al diseño de taxonomías, y deja abiertas las preguntas de hasta qué punto puede reutilizarse el trabajo ya hecho en taxonomías imperfectas en el campo de la seguridad informática al diseñar otras nuevas.

El trabajo presentado por Lough 2001 no es formalmente una comparación de taxonomías, aunque justificando el desarrollo de su propia taxonomía incluye una extensa revisión del campo, revisando en su tercer capítulo 16 taxonomías de ataques que pueden realizarse contra computadoras, y en el cuarto, las cuatro principales utilizadas para caracterizar fallos en los sistemas operativos. En el transcurso de su trabajo, realiza extensivas comparaciones y busca equivalencias, demostrando que la descripción de tipos de ataque (o de las debilidades que los ataques aprovechan) son en gran medida equivalentes, que el espacio cubierto por éstas tiene una gran superposición.

La revisión realizada en el trabajo de Lough es muy extensa, pero –al igual que el caso anterior– resulta muy antigua para su aplicación actual. Lough presenta una nueva taxonomía, a la que denomina VEREDICT (*Validation Exposure Randomness Deallocation Improper Conditions Taxonomy*), integrando los puntos más sobresalientes de veinte años de desarrollos en el campo, pero su enfoque principal es la aplicación a ataques en redes inalámbricas.

El trabajo de Polepeddi 2005 está motivado por la existencia de bases de datos grandes y de acceso público que cubren distintos aspectos importantes de las vulnerabilidades conforme van apareciendo, pero que dadas sus diferencias tanto en cuanto a los objetivos que persiguen como a la metodología que siguen dificultan la comparación cruzada entre casos de vulnerabilidad. Polepeddi busca «consolidar las taxonomías de vulnerabilidades de software de forma inambigua» para facilitar un acceso a la información completa de todos los aspectos de una vulnerabilidad, orientando a una minería de datos efectiva, que genere resultados «repetibles, inambiguos y exhaustivos».

Polepeddi clasifica las cinco principales bases de datos de vulnerabilidades (BugTraq, ICAT, OSVDB, Computer Associates' VIC y Secunia), seleccionadas a partir de la cobertura que dan a los seis principios que menciona Amoroso 1994 como requisitos para una taxonomía (subconjunto de los que fueron listados al principio de la presente sección). El trabajo llega únicamente a la conclusión de que «es posible crear una taxonomía consolidada que cubra y organice todos los datos relevantes», y apunta a algunos hitos que tendrían que cruzarse para lograrlo (particularmente, dedica un largo argumento a la ubicación de una *llave primaria* para referirse a los datos), pero excede al ámbito de su trabajo presentarla.

Igure y Williams 2008 presentan un trabajo dividido claramente en dos mitades claramente distintas — En primer lugar, presentan un listado con 18 taxonomías de ataques, y en segundo lugar, uno con 16 taxonomías de vulnerabilidades. Su exposición inicia reconociendo la dependencia mutua entre ambas, pero sus fundamentales diferencias: «La evaluación de seguridad de un sistema es el proceso de determinar su capacidad de resistir ataques. Este proceso típicamente involucra probar el sistema para detectar la presencia de vulnerabilidades conocidas que no hayan sido corregidas» (traducción propia). Sin embargo, lo que buscan clasificar unos y otros es tan distinto, que los autores encuentran valor en presentar sus resultados por separado.

Igure y Williams describen una tras otra las taxonomías que estudian, cubriendo 20 años de literatura científica en lo referente a ataques y 30 años en las vulnerabilidades. Presentan dos cuadros resumiendo su experiencia, indicando para cada taxonomía los objetivos que ésta persigue, qué dimensiones la caracterizan (esto es, cómo se ve *a vuelo de ave* el modelo de representación propuesto por la taxonomía) y comentarios adicionales para cada una; adoptamos este mismo formato para el Cuadro 5.1.

El estudio de Igure y Williams también condujo indirectamente a que se decidiera incluir como taxonomía el trabajo de Regenscheid y Hastings 2008 a pesar de no serlo formalmente, como se menciona al inicio de la Sección 2.4.3: Un trabajo que no se presenta como taxonomía, pero cumple con las características de una, y ofrece un punto de vista diferente y más acorde a determinada necesidad, puede evaluarse (y probablemente

implementarse) en el contexto de una taxonomía.

Hui y col. 2010 se enfoca en los defectos de seguridad en el software. Inicia exponiendo los diferentes términos utilizados por la IEEE que pueden caber en la definición general de *defecto* (*error*, acción humana que produce un resultado incorrecto; *falla*, un paso, proceso o definición de datos incorrecta en un programa, y *fallo*, la incapacidad de un sistema o componente para cumplir con las funciones que le son requeridas dentro de determinados requisitos) para explicar cómo un *defecto en seguridad en el software* se puede convertir en una *vulnerabilidad en el software* si hay un punto de inserción de datos desde donde se pueda explotar. Esta vulnerabilidad se convierte en una *amenaza de seguridad en el software* cuando es descubierta, y una vez explotada se vuelve un *accidente de seguridad en el software*.

Continúa con un recorrido histórico sobre las taxonomías empleadas para estudiar las vulnerabilidades desde la década de los setenta y por más de 30 años, presentando los puntos principales de nueve taxonomías. Además, presenta una tabla indicando el principal objetivo, motivación e insuficiencias que encontraron en cada una de las estudiadas.

Tripathi y Singh 2010 presenta brevemente catorce taxonomías explicando el enfoque principal de cada una de ellas como paso necesario para avanzar hacia la estandarización en taxonomías de vulnerabilidades; su trabajo es motivado por la frustración ante la gran cantidad de taxonomías existentes cubriendo un mismo espacio de problematización. Dado que, al igual que los demás trabajos, presenta un listado cubriendo más de treinta años de avances, menciona que si bien muchas de las taxonomías «sirven a distintos propósitos y son útiles para sus fines propuestos, están desactualizadas y resultan de uso muy limitado». Reconoce, a pesar de la importancia de actualizar las taxonomías históricas, resulta un emprendimiento muy difícil por el ritmo de cambio; esto deja al espacio que cada una de éstas llenaba como incompleto o vacío. Apunta a iniciativas como los proyectos de MITRE, PLOVER (Christey 2006) y CWE (Martin y Barnum 2008), como iniciativas que requieren la asistencia de una buena taxonomización automatizable y generalizada.

Joshi, Singh y Tarey 2015 parte de los mismos razonamientos y motivaciones comunes que el estudio mencionado anteriormente (de hecho, ambos estudios comparten a uno de los coautores). Presenta a 25 taxonomías, siendo su núcleo una tabla en que las presenta sobre tres columnas, mas una de comentarios: El esquema de clasificación (unidimensional, en capas, jerárquico, multidimensional), una sucinta descripción del atributo clasificador central, y el objetivo primario que persigue.

3.2. Comparativas de experiencias en la aplicación del voto electrónico

El presente trabajo parte de la clasificación de 24 casos en que hubo algún tipo de fallo en la aplicación de esquemas de voto electrónico. Habiendo presentado ya el estado del arte en lo relacionado a estudios que comparan taxonomías relativas a la seguridad informática, a continuación se abordan estudios relacionados al voto electrónico. Dado que el tema ha sido abordado desde ángulos tan distintos, los estudios se presentan organizados según la disciplina primaria en que se enmarca cada uno de ellos.

3.2.1. Humanidades y ciencias sociales

Como se mencionó en la introducción, siendo la emisión del voto un hecho tan importante para la sociedad, su estudio cruza problemas que atañen a muy distintas disciplinas. Pero, como también se menciona ya desde ahí, hay una desconexión entre dichos campos, llevando a una *mutua incredulidad* respecto a los resultados

que uno y otro campos apuntan.

Romero Flores y Téllez Valdés 2010 presentan un trabajo escrito a partir del derecho (sin ir más lejos, titulado *«Voto electrónico, derecho y otras implicaciones»*) en que intentan presentar una visión general. Presentan la adopción de un esquema de voto electrónico casi como un hecho inevitable, una tendencia positiva hacia la cual se debe transitar:

> Es inevitable la tendencia creciente de los organismos electorales de utilizar la informática electoral en actos previos a los comicios, durante la jornada electoral y en actos posteriores a la actividad comicial, razón por la que es inaplazable, en materia electoral, contar con todas las hipótesis legales que pueden desprenderse del propio uso de la informática electoral, especialmente de las urnas electrónicas.

Uno de los principales potenciales problemas que Romero y Téllez ven a la adopción del voto electrónico es la resistencia de la sociedad por el distinto nivel de acceso a la tecnología derivado en buena medida del nivel socioeconómico, cultural y etáneo:

> El ser humano, frente a las nuevas tecnologías de la información y comunicación, está condicionado, en principio, a factores de índole económica; es innegable que el poseer mayores recursos facilita el acceso a las TIC (...) La educación tiene suma importancia en relación con el estatus. Recordemos que en la mayoría de las sociedades actuales el estatus se relaciona directamente con los logros intelectuales. (...) es decir, la diferencia ahora es entre alfabetos digitales y analfabetos digitales. (...) Las nuevas generaciones de seres humanos, prácticamente han crecido y se han desarrollado dentro de un ámbito tecnológico (...) Este proceso resulta menos difícil para la gente joven respecto de las personas mayores, con lo cual se presenta una brecha generacional tecnológica a partir de la edad.

Dada la disciplina de origen de Romero y Téllez, su texto cuenta con un relato completo y muy interesante de las discusiones legislativas que llevaron a que en las sucesivas leyes electorales mexicanas entre 1911 y 1977 se previera positivamente el uso de sistemas automatizados (mecánicos) para la emisión del sufragio, así como las principales razones para que el Código Federal Electoral de 1987 lo suprimiera.

El trabajo de Romero y Téllez concluye con un extenso apéndice, un cuadro de veinte páginas de extensión, enumerando 139 experiencias entre 1985 y 2009 (enfocándose particularmete en el periodo 2002-2006, que reúne 92 de las entradas). Para cada uno de los casos descritos presenta las siguientes columnas:

- País / organismo
- Periodo
- Tipo de elección / modalidad
- Proveedora de la solución tecnológica
- Número de electores participantes
- Marco legal
- Efectos de la experiencia

Desafortunadamente, en aras de presentarse de forma exhaustiva, la información que forma parte de esta tabla no puede verse como una comparativa — El ordenamiento no es claro: Se presentan agrupados por regiones (56 de América Latina, 65 de Europa, 12 de Asia y 6 del resto del mundo), y dentro de cada una de éstas, ordenados por nombre del país, aunque de forma inconsistente, y sin un claro ordenamiento secundario. Presenta información incompleta para obtener mayores detalles respecto a cada una de las experiencias citadas (por ejemplo, en numerosas ocasiones omite el año), y no hay una indicación clara de por qué una experiencia está o no enlistada; no se presenta esto como una crítica contra el trabajo de Romero y Téllez como un todo; queda claro que este listado es meramente un apéndice y no fundamental al trabajo que presentan.

Soldevilla 2004 es publicado como parte de un libro de la ONPE (autoridad electoral de Perú), y es escrito en uno de los momentos de mayor efervescencia y aparente inevitabilidad de la adopción del voto electrónico. Menciona que:

> En América Latina tanto los electores como las organizaciones políticas exigen de los organismos electorales tres puntos que cada vez se tornan más rigurosos: Eficiencia en el servicio de votación; confianza en las entidades electorales, que deben estar exentas de velos, atmósferas turbias y cualquier indicio que pueda delatar fraude o manipulación; y resultados inmediatos. (...) La tecnología informática al servicio de las elecciones debe mantener estos principios para obtener legitimidad. Una de las soluciones informáticas propuestas ha sido la implementación del voto electrónico, automatizando el sufragio.

En su apartado de *las dificultades*, menciona como principal obstáculo del voto electrónico la aceptación por parte de una sociedad con escaso contacto con la tecnología, planteando a la capacitación como cura para esta oposición:

> (...)los mecanismos de votación electrónica pueden parecer como perjudiciales para las poblaciones analfabetas o vernáculo-parlantes; sin embargo, todo indica que la enorme riqueza visual que ofrecen estas opciones de votación puede facilitar los correspondientes procesos de capacitación. (...) Un tema crucial es el elector, cuyo nivel cultural y escolaridad varían. En muchos casos se señala que, si es difícil para muchos electores entender cómo votar en el sistema manual, los problemas que surgirían al tentar una votación electrónica resultan desbordantes. (...)

Resulta curiosa y digna de destacarse la opinión de Soldevilla ante el avance de equipos DRE hacia VVPAT:

> La auditabilidad del voto electrónico es el tema central en algunos procesos de implementación del voto electrónico (caso de EE.UU., no así Brasil). Por ejemplo, en EE.UU. se está divulgando un procedimiento de auditabilidad del voto electrónico que hace que la máquina de votación electrónica imprima el voto y lo deposite para un posterior conteo de verificación. Esta errónea concepción proviene de una vieja práctica de los contadores y auditores contables que señala que toda transacción debe dejar rastro en papel. (...) El tema de los *hackers* (...) constituyen las principales preocupaciones de los actores electorales implicados. Para la intrusión externa en un proceso electoral realizado con votación electrónica, el *hacker* debe contar con una «puerta de entrada», un punto de red vía internet o módem que lo conecte con la red de votación de las mesas de votación. El sistema propuesto por los organismos electorales no contempla ninguno de estos

> puntos de acceso, por lo que esta intrusión sería nula al momento de efectuarse el acto de votación. Más tarde, en la etapa de transferencia de datos, los organismos electorales implementan una Red Privada Virtual, que corre de forma paralela a la red mundial por la que discurre Internet.

El apartado parcialmente citado incurre en una cantidad peligrosa de errores técnicos, ilustrando desde el otro lado lo ya dicho: El problema de la seguridad de todo esquema de voto electrónico requiere no únicamente de su estudio por expertos en una disciplina, sino que de un trabajo interdisciplinario.

Soldevilla presenta un cuadro en que compara los marcos legales en cuestión electoral de los países latinoamericanos, indicando en cada caso si la legislación requiere expresamente el uso de una *boleta* o *papeleta* electoral, si prohíbe la votación electrónica, y si hace referencia explícita al voto electrónico; concluye que ninguno de los países de la región la prohíbe expresamente. Por último, hace un recorrido aproximadamente cronológico sobre la adopción de voto electrónico en el mundo (10 experiencias en Latinoamérica y 13 en el resto del mundo). Si bien este es presentado como un relato textual, y no como un cuadro comparativo donde se puedan buscar visualmente patrones o tendencias, resulta interesante que presenta los hitos legislativos que muchos de estos países han cruzado.

3.2.2. Ciencias e ingeniería de la computación

La reconocida tesis doctoral de Mercuri 2001 dedica la Sección 1.5 al estudio de *casos ilustrativos*; presenta 8 casos, todos ellos ocurridos en los Estados Unidos entre los años 1992 y 2000. Mercuri se limita a presentar dichos casos como parte de su introducción, explicando por qué elabora su propuesta; no la presenta como una comparativa. Citamos aquí al trabajo de Mercuri por varias razones: En primer lugar, por ser uno de los primeros realizados a esta profundidad en el tema del voto electrónico desde la perspectiva de la seguridad informática, pero también en buena medida por explicitar la *multidisciplinareidad* requerida para abordar el problema. Su capítulo 4 está dedicado a los aspectos sociológicos de la elección, e inicia con la siguiente reflexión (traducción propia):

> Los aspectos sociológicos, que pueden parecer «ligeros» desde el punto de vista de las ciencias de la computación, frecuentemente proveen información en razón de la seguridad y diseño del sistema (...) La percepción del votante respecto a si su voto efectivamente «contó» es un factor principal en la participación en el día de la elección. (...) Analizamos los aspectos de negocios relacionados con las elecciones, y describimos las técnicas para el mal uso que pueden emplearse para subvertir el proceso de tabulación de los votos.

En dicho capítulo, proporciona varias citas y cifras respecto a por qué la jornada electoral en los Estados Unidos es, en toda forma, un negocio redondo, y menciona:

> Si se ve como negocio, suena a negocio y huele a negocio, el negocio electoral seguirá, con toda probabilidad, operando bajo la tradicional ley de la oferta y la demanda. (...) Si este es realmente el caso, los votantes (o quienes compran sistemas de votación) desearán que el proceso siga sin ser asegurado, y se sigan creando y vendiendo sistemas que provean de oportunidades de robar una elección. (...) De forma alternativa, si el público demanda que los sistemas electorales sean sujetos de regulaciones y escrutinio similares a los que se aplican a otros negocios que dependen de la confianza pública (...), procedimientos rigurosos de estandarización y cumplimiento podrán comenzar a desarrollarse y aplicarse.

Mercuri explica por qué toma al análisis del voto electrónico más como la aplicación de la seguridad informática a un enfoque social que a uno algorítmico:

> La criptografía intenta pasar como una solución tecnológica (algorítmica) a un problema sociológico (privacidad), y promueve falsas garantías por parte de desarrolladores, legisladores, y otros quienes promueven dichos productos. Esta afirmación peca de ambiciosa, ya que viene de darnos cuenta dentro de la industria del cómputo que la criptografía, por sí misma, no provee una solución de sistema seguro. El conocido criptógrafo Bruce Schneier recientemente retractó su máxima anterior, «no es suficiente protegernos con leyes; debemos protegernos con matemáticas». Hoy afirma que la criptografía no es una «bala mágica», diciendo:
>
> «He creado mi carrera como un consultor en criptografía: Diseñando y analizando sistemas de seguridad. Para mi sorpresa inicial, encontré que los puntos débiles no tenían nada que ver con las matemáticas. Estaban en el hardware, en el software, en las redes, en la gente. Desarrollos matemáticos hermosos fueron hechos irrelevantes mediante una mala programación, un sistema operativo de segunda, o la mala elección de contraseñas de alguien.»

Places Chungata y col. 2017 hace una breve revisión del estado de avance de la adopción del voto electrónico en el mundo, buscando insertar a Ecuador en éste. Presentan un listado seccionado en tres por grado de avance (*Implantados* con siete casos: dos casos en Europa, tres en América y dos en Asia; *Estudio o implantación parcial* con 18 casos: cuatro en Europa, uno en África, nueve en América, tres en Asia y uno en Oceanía, *Legalmente prohibido o paralizado*, con cinco casos, todos ellos en Europa). Presenta una breve reseña de la experiencia electoral en dichos países, indicando las fechas de los principales hitos que se observan en cada uno. Realiza además una descripción más a fondo de las experiencias piloto que se han sostenido en el Ecuador.

3.2.3. Interdisciplina y divulgación

El estudio que coordinan y presentan Busaniche y Heinz 2009 constituye un libro claramente crítico a toda implementación de voto electrónico, definiéndolo como:

> En un sentido estricto denominaremos aquí «voto electrónico» a los mecanismos diseñados para emitir y contar los sufragios en un único acto, a través de algún sistema informático instalado y en funcionamiento en el lugar mismo donde el elector concurre a expresar su voluntad política.

El libro presenta, después de una presentación de distintos aspectos relacionados en cuatro pequeños capítulos; un apartado titulado *Voces*, que recoge las experiencias de cinco personas implicadas en las experiencias de voto electrónico en Argentina, en las localidades de Ushuaia (provincia de Tierra del Fuego) en 2003, Las Grutas (provincia de Río Negro; ver Sección 4.3.5) en 2007, y las tentativas de adopción en la Ciudad Autónoma de Buenos Aires en 2008; otro apartado titulado *Ensayos*, con reflexiones críticas de seis expertos, mayormente académicos de las áreas de ingeniería y matemáticas de universidades argentinas y brasileñas, así como el de la coordinadora del proyecto Beatriz Busaniche (politóloga argentina). Por último, una sección en que presentan cinco experiencias internacionales de falla del voto electrónico; los casos que aborda incluyen a los que este trabajo aborda en las Secciones 4.3.4, 4.3.9 y 4.3.7.

El trabajo de Busaniche y Heinz ha sido de gran importancia social en Argentina; si bien es un libro corto y no sigue el rigor de las publicaciones formales, resultó importante para nuclear una importante

comunidad nacional de opositores a la adopción de una modalidad específica voto electrónico que ha avanzado fuertemente desde el 2014; muestra de ello son los casos descritos en las Secciones 4.3.20 y 4.3.21.

En lo relativo al aporte del texto de Busaniche y Heinz al trabajo actual, claramente es un punto de partida, sin embargo la cobertura que realiza del tema, al mantenerse dentro del terreno de los ensayos y de la divulgación no puede ser aprovechada más a fondo. Respecto a la lista de casos que presenta, no los aborda de forma comparable, sino que reproduce notas periodísticas con las que se dio a conocer cada uno de ellos.

El texto antes mencionado fue antecedente directo de mi involucramiento personal en el tema. En Wolf 2011 se presentan las supuestas ventajas principales del voto electrónico (disminución de costos, agilidad en la obtención de resultados, confiabilidad de los actores) como falacias dada la experiencia internacional, y se presentan diez casos de fallos (todos los cuales son recogidos y presentados en este trabajo). Dicho texto, al igual que el anterior, se limita a presentar un grupo de fallos, sin clasificarlos ni verlos de forma integral.

Capítulo 4

Clasificación de los casos estudiados

La investigación se centró en el análisis de 24 casos de fallos diversos aspectos de sistemas de votación electrónica, en el periodo comprendido entre 2004 y 2015. Las fuentes de información de dichos casos son mayormente artículos periodísticos refiriendo al suceso en cuestión, lo cual limita fuertemente la cantidad de información disponible para su análisis.

Los 24 casos que se presentan a continuación fueron inicialmente clasificados mediante un etiquetado temático abierto, antes de abordar la clasificación mediante taxonomías; si bien el etiquetado simple carece de método como para elaborar conclusiones fuertes al respecto, se presenta como punto de dato comparativo, y la información que puede obtenerse del conjunto se aborda en la Sección 5.1.

4.1. Descripción del estudio realizado

Una vez identificados los 24 casos a estudiar y obtenida la información relevante de ellos, se realizó un etiquetado temático abierto, así como uno limitado al tipo de fuente del cual se obtuvo la información de cada fallo. Los cinco tipos definidos para este etiquetado son:

Periodístico Cobertura realizada por algún medio noticioso.

Adversarial El fallo es encontrado, documentado *y divulgado* por una persona o equipo *ajenos* a la autoridad electoral, actuando sin autorización de la misma, y típicamente buscando desacreditarla de alguna manera.

Auditoría Cuando un reporte de fallo documenta el proceso descubierto al realizar una auditoría, prueba de penetración, análisis forense o cualquier otro *con la anuencia* de la autoridad electoral.

Reporte Indica que la autoridad electoral fue notificada de un fallo lo suficientemente grave como para que realice un estudio al respecto y presente un reporte con sus conclusiones.

Comparecencia Si el caso fue dado a conocer por las declaraciones de algún actor implicado, en el transcurso de una audiencia pública.

Además de estos dos etiquetados, se presenta la categorización sobre las tres taxonomías antes descritas, y empleando las representaciones sugeridas en la Sección 4.2. La comparación y análisis de los datos obtenidos a lo largo del presente capítulo se presentará en el capítulo 5.

4.1.1. Ámbito del trabajo

Es necesario acotar explícitamente lo que se considera dentro o fuera del ámbito del presente trabajo. De las modalidades de votación presentadas en la Sección 2.3, se considera dentro del ámbito de trabajo a los esquemas de votación en que *la voluntad del elector es inmaterializada*, esto es, convertida en una expresión electrónica e intangible, y almacenada en un dispositivo electrónico. Esto es, de entre las modalidades recién descritas, se estudian casos derivados de la aplicación de:

1. Urnas electrónicas
    a) DRE
    b) VVPAT
    c) Boleta electrónica
2. En ausencia
    a) Voto en línea

Es importante recalcar que, si bien los sistemas VVPAT cuentan con la emisión de comprobantes o *testigos* del voto, en muchos casos resultan inútiles dado que la *verdad legal* está definida como el resultado obtenido de la memoria del dispositivo.

Cabe mencionar que las urnas mecánicas también entrarían en la delimitación presentada, sin embargo, siendo tecnología con más de un siglo de antigüedad, y estando ya en franco proceso de abandono y desaparición en los Estados Unidos (único país que las adoptó a gran escala), no se consideran ya relevantes para la investigación.

También se explicita que, por economía de palabras, en el transcurso del trabajo se hará referencia a la *votación tradicional* sobreentendiendo que se hace referencia a los sistemas de emisión de votación en papel, esto es, el conjunto de *boleta partidaria o sábana*, *boleta única o australiana*, *lectura óptica* y *tarjetas perforadas*.

4.2. Representación visual de las taxonomías

Dada la naturaleza de las taxonomías aplicadas, en que se presenta un conjunto de datos de forma binaria (representando la presencia o ausencia de ciertas características, esto es, si un dado vector de la categoría está involucrado en cada caso estudiado), para la primera (7RP) y tercera (AASVU) se decidió representar la categorización empleando gráficas de *radar* (también conocidas como de *estrella*) (Croarkin 2012, Sección 1.3.3.29); para la segunda taxonomía abordada (ROdC), dado que está estructurada jerárquicamente, se eligió un *diagrama de carámbanos* (*icicle diagram*), presentado por legibilidad con la raíz del lado izquierdo (Heer, Bostock y Ogievetsky 2010, Figura 4D).

En las siguientes secciones se presentan las particularidades de representación para cada taxonomía.

4.2.1. 7RP: Siete Reinos Perniciosos

En la Figura 4.1 puede apreciarse un ejemplo de evaluación basado en 7RP: Este diagrama, correspondiente al caso que se presentará en la sección 4.3.4, indica que el problema se debió a factores de hardware y a las características de seguridad del sistema. Saltará a la vista de inmediato que no son siete u ocho vectores

de clasificación, como podría esperarse, sino que once. En la evaluación a la presente taxonomía realizada en la Sección 5.2 se justifica por qué se consideró necesario agregar las siguientes tres categorías:

- No clasificable
- Hardware
- Humano

Estas tres categorías están indicadas con un asterisco en las gráficas.

Figura 4.1: Ejemplo de análisis de un caso empleando la taxonomía 7RP

4.2.2. ROdC: Riesgos Operacionales de Ciberseguridad

La jerarquización que presenta esta taxonomía resulta muy interesante para mantener y representar en nuestros resultados; los diagramas generados representan los tres niveles de acercamiento de izquierda a derecha; la clasificación se realizó sobre el nivel más específico (derecha), y una categoría se marca como *activa* si cualquiera de sus subcategorías lo está.

Se presentan todas las categorías, con un color de fondo obscuro indicando presencia, y fondo claro indicando ausencia.

La Figura 4.2 muestra al ejemplo de evaluación correspondiente a la Sección 4.3.4: En el apartado *acciones de personas*, se refiere a un caso inadvertido por omisión (1.1.3), que redunda en tres por inacción (por falta de habilidades, 1.3.1, de conocimiento, 1.3.2 y de guía, 1.3.3). Además de esto, se identifican problemas derivados de fallas en sistemas y tecnología: Por parte del hardware, la obsolescencia (2.1.4); por parte del software, la configuración de seguridad (2.2.4), y por parte de los sistemas, fallas de diseño (2.3.1) y de especificaciones (2.3.2).

4.2.3. AASVU: Análisis de Amenazas en Sistemas de Votación UOCAVA

La categorización que presenta este esquema, a diferencia de aquellas pensadas directamente para emplearse como taxonomías, presenta varios vectores que pueden representarse de forma binaria, pero agrega dos (*esfuerzo requerido* y *facilidad de detección*) que pueden ocupar uno de tres niveles (bajo, medio y alto).

Figura 4.2: Ejemplo de análisis de un caso empleando la taxonomía RoDC

Cuadro 4.1: Niveles de esfuerzo requeridos para un ataque bajo la representación de la taxonomía AAVSU (traducción propia).

Nivel	Descripción	Ejemplo
Bajo 	Un ataque requeriría pocos o limitados recursos o conocimiento detallado del sistema.	Forzar a un votante a votar de cierta manera mediante la presencia del atacante.
Medio	Un ataque requeriría recursos significativos (o la capacidad de obtenerlos) o conocimiento del sistema. En esta categoría entran los ataques internos involucrando a un pequeño número de conspiradores.	Negación de servicio (DoS) contra las computadoras y servidores oficiales de la elección.
Alto 	Un ataque requeriría recursos extraordinarios, conocimiento del sistema, o acceso al sistema. En esta categoría entran los ataques internos que involucran a una gran cantidad de conspiradores.	Reemplazar las boletas emitidas por voto postal durante un recuento manual.

Cuadro 4.2: Niveles de facilidad de detección bajo la representación de la taxonomía AAVSU (traducción propia).

Nivel	Descripción	Ejemplo
Baja 	La probabilidad de detectar un ataque es muy baja sin recursos extraordinarios.	Código malicioso instalado en el equipo electoral por el personal interno.
Media	Un ataque podría ser detectable, pero requeriría una gran cantidad de recursos y tiempo. Es poco probable detectar este tipo de ataques durante la elección.	Un virus informático infectando computadoras personales involucradas.
Alta 	Un ataque sería probablemente detectado dado un monitoreo correcto.	Un atacante dirige a los votantes a un sitio electoral impostor.

Dado que todo caso tendrá un valor en esta escala, y que estos puntos califican directamente la severidad de cada uno de los casos abordados, se tomó la poco ortodoxa decisión de *agregar* a la gráfica de radar dos iconos que la *califican*, dándole una ayuda visual y color distintivo a cada uno de los casos; naturalmente, se da mayor severidad al *bajo esfuerzo* para efectuar un ataque, así como a la *baja facilidad* para detectarlo. Los iconos en cuestión son presentados en los Cuadros 4.1 y 4.2.

Resulta pertinente apuntar que los dos vectores mencionados se prestan a la confusión: El nivel de esfuerzo resulta bastante intuitivo (un ataque muy complejo puntearía como de *alto esfuerzo* en tanto que un error de funcionamiento observado sería de *bajo esfuerzo*, dado que probablemente ni siquiera hubo intencionalidad detrás de él), se observó en el desarrollo del presente trabajo que varias personas se confundían al presentárseles que un caso resulta de *baja facilidad de detección* (es difícil darse cuenta que ocurrió) o *alta facilidad de detección* (es trivial detectarlo).

El empleo de indicadores icónicos para estos dos apartados ayudan particularmente a su comprensión.

La Figura 4.3 presenta la evaluación que se realizará de caso que se presenta en la Sección 4.3.4: El ataque compromete las propiedades de *integridad* y de *confidencialidad*, y puede ser efectuado por un *individuo hostil*

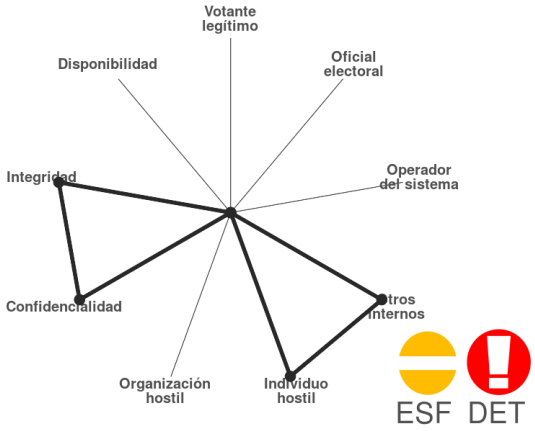


Figura 4.3: Ejemplo de análisis de un caso empleando la taxonomía AASVU

y por *otros usuarios internos*; el esfuerzo requerido para llevar a cabo este ataque es considerado *mediano* (si bien resulta muy fácil y barato hacerse de una llave, utilizar este acceso para modificar el estado o la programación del sistema requeriría de conocimiento del sistema en cuestión), y la facilidad de detección es *baja* (resultaría casi imposible detectar que un ataque de este tipo hubiera ocurrido).

4.3. Aplicación de las taxonomías

A continuación se presenta a cada uno de los 24 casos abordados, uno por página. La presentación se hace siguiendo un orden cronológico para facilitar su revisión rápida; a nivel estructural del documento, cada caso se presenta como una subsección para facilitar su referenciación.

Cada uno de los casos que se presentan a continuación inician con una breve descripción de lo ocurrido, la indicación del tipo de fuente de información utilizado y las etiquetadas resultantes del proceso de etiquetado abierto, y la representación sobre cada una de las taxonomías como lo describe la Sección 4.2. Del lado izquierdo se presentan las gráficas correspondientes a 7RP y AAVSU, y del lado derecho la tabla correspondiente a ROdC.

4.3.1. Ohio, EUA, 2004

El programador Clinton Eugene Curtis testificó bajo juramento, relatando su experiencia diseñando un sistema para robar votos para la elección en Florida, 2000, bajo las órdenes del legislador local Tom Feeney. En el testimonio indica que, basado en su experiencia, la desviación entre los datos de encuestas de salida y la votación recibida oficialmente en el estado de Ohio en 2004 apuntaría a un probable fraude. Explica también algunas técnicas que pueden utilizarse para esconder el código incluso de una auditoría. (Curtis 2004)

Fuente Comparecencia

Etiquetas Fraude, confesión

Figura 4.4: Caso 1 evaluado bajo 7RP

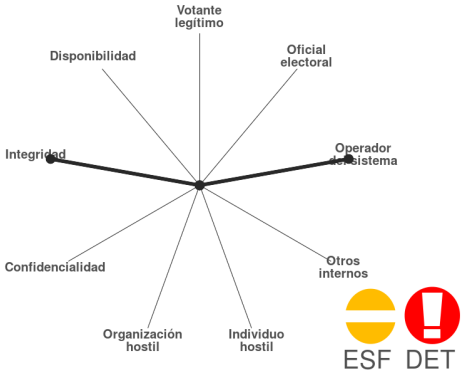


Figura 4.5: Caso 1 evaluado bajo AAVSU

Procesos externos	Dependencias de servicio	Transporte
		Combustible
		Servicios de emergencia
		Utilidades
	Problemas de negocio	Condiciones económicas
		Condiciones del mercado
		Falta de suministros
	Problemas legales	Litigación
		Legislación
		Cumplimiento regulatorio
	Desastres	Pandemia
		Descontento
		Terremoto
		Inundación
		Fuego
		Evento climático
Procesos internos fallidos	Soporte	Adquisición
		Capacitación y desarrollo
		Fondeo
		Personal
	Controles	Propiedad del proceso
		Revisión periódica
		Métricas
		Monitoreo de estado
	Diseño o ejecución	Entrega de tareas
		Acuerdos de nivel de servicio
		Escalación de problemas
		Flujo de información
		Notificaciones y alertas
		Papeles y responsabilidades
		Documentación de procesos
		Flujo de procesos
Fallas de sistemas y tecnología	Sistemas	Complejidad
		Integración
		Especificaciones
		Diseño
	Software	Pruebas
		Prácticas de codificación
		Configuración de seguridad
		Control de cambios
		Administración de configuración
		Compatibilidad
	Hardware	Obsolescencia
		Mantenimiento
		Rendimiento
		Capacidad
Acciones de personas	Inacción	Disponibilidad
		Guía
		Conocimiento
		Habilidades
	Deliberado	Vandalismo
		Robo
		Sabotaje
		Fraude
	Inadvertido	Omisiones
		Errores
		Equivocaciones

Figura 4.6: Caso 1 evaluado bajo ROdC

4.3.2. EUA, California, 2004

Kevin Shelley, secretario de Estado de California, *des-certificó* y prohibió el uso de ciertos modelos de urnas electrónicas Diebold en los condados de Solano, San Joaquín, Kern y San Diego, y ordenó a 10 condados adicionales dar pasos para mejorar la seguridad y confiabilidad de dichos equipos (Lucas 2004), al descubrirse que el software cargado en dichas urnas no era el mismo que el que se había sometido para certificación.

Fuente Periodístico

Etiquetas Diebold, verificación, concordancia

Figura 4.7: Caso 2 evaluado bajo 7RP

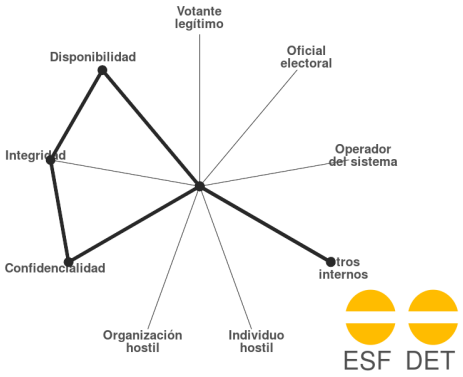


Figura 4.8: Caso 2 evaluado bajo AAVSU

Figura 4.9: Caso 2 evaluado bajo ROdC

4.3.3. Montreal, Canadá, 2005

Fallos de las urnas llevaron a que unos 45,000 votos fueran contabilizados doblemente, llevando a la anulación de la elección. La Dirección General de Elecciones de Quebec realizó un estudio (DGEQ 2006), apuntando a las principales causas del fallo: Falta de acceso al código fuente, pruebas de funcionalidad, plan de contingencia, medidas estrictas de almacenamiento y resguardo de los equipos.

Marcel Blanchet, funcionario electoral en jefe opinó que "las urnas y terminales de votación electrónicas son tecnologías vulnerables. Más allá de la manera en que fueron manejadas, no ofrecen suficiente garantía de transparencia y seguridad para asegurar la integridad del voto". (Geist 2006)

Fuente Reporte

Etiquetas Integridad, código fuente, resguardo, plan de contingencia

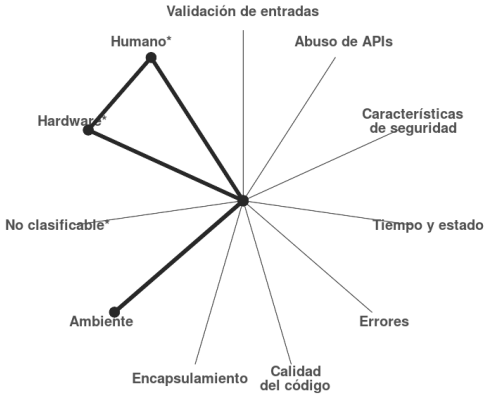


Figura 4.10: Caso 3 evaluado bajo 7RP

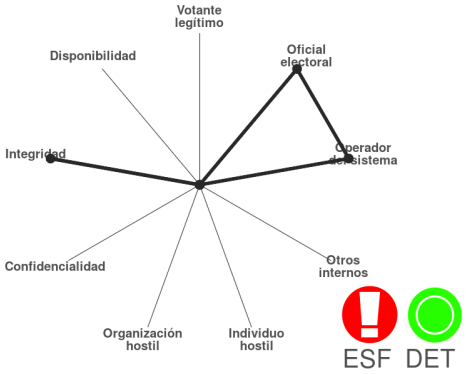


Figura 4.11: Caso 3 evaluado bajo AAVSU

Figura 4.12: Caso 3 evaluado bajo ROdC

4.3.4. EUA, 2006

El investigador Ed Felten encuentra que la cerradura empleada por las urnas electrónicas *Diebold AccuVote-TS* para proteger el acceso a la tarjeta de memoria donde se almacenan los votos es una llave genérica (e idéntica) empleada para archiveros de oficina, minibares de hotel y *rockolas*; estas llaves pueden comprarse al por mayor en línea, y no proporcionan seguridad física real alguna. (Felten 2006)

Fuente Adversarial

Etiquetas Diebold, Falsa seguridad

Figura 4.13: Caso 4 evaluado bajo 7RP

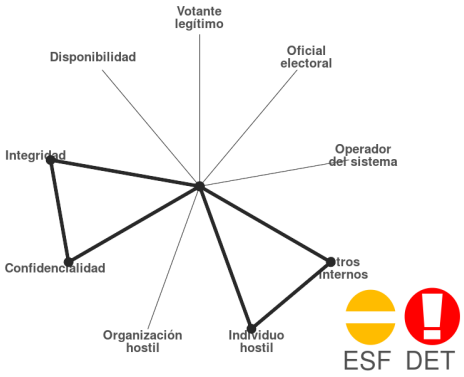


Figura 4.14: Caso 4 evaluado bajo AAVSU

Figura 4.15: Caso 4 evaluado bajo ROdC

4.3.5. Río Negro, Argentina, 2007

Se hizo un piloto de votación electrónica para la mitad de las mesas electorales de la localidad de Las Grutas, provincia de Río Negro. Se presentaron discrepancias entre padrón electoral "oficial" y digital; aproximadamente 40 % de los votantes no aparecieran con derecho a sufragar, con lo cual las autoridades de mesa tuvieron que registrar a dichos votantes en la mesa contigua (que operaba con voto en papeletas). Además de esto, al obtener el cómputo de votos al final de la jornada, un error de operación llevó a la eliminación de los resultados completos de una mesa (emitió un comprobante con cero votos registrados). (Busaniche 2007)

Fuente Adversarial

Etiquetas Usabilidad, padrón, discrepancia

Figura 4.16: Caso 5 evaluado bajo 7RP

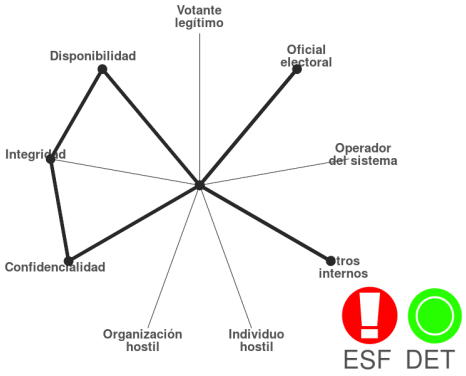


Figura 4.17: Caso 5 evaluado bajo AAVSU

Figura 4.18: Caso 5 evaluado bajo ROdC

4.3.6. Nueva Jersey, EUA, 2008

Tras las elecciones primarias de 2008, Ed Felten documentó varias decenas de actas de totalización de resultados emitidas por urnas electrónicas *Sequoia AVC Advantage* en las que el total de votos emitidos no es igual a la suma de los votos emitidos por cada una de las opciones. (Felten 2008)

Al darse a conocer este caso, oficiales electorales del Estado de Nueva Jersey ofrecieron enviar a Felten una de las urnas electrónicas que exhibieron el comportamiento anómalo para su análisis independiente, a lo cual la empresa respondió con amenazas de denuncia, pues esto violaría el contrato de uso del equipo.

Fuente Adversarial

Etiquetas Integridad, error aritmético

Figura 4.19: Caso 6 evaluado bajo 7RP

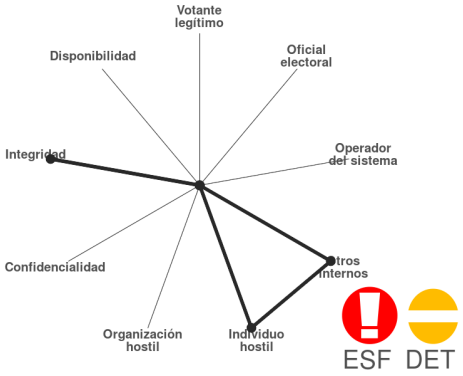


Figura 4.20: Caso 6 evaluado bajo AAVSU

Figura 4.21: Caso 6 evaluado bajo ROdC

4.3.7. EUA, 2008

Las urnas electrónicas empleadas para las elecciones presidenciales de 2008 en los Estados de Pennsylvania, Virginia, Michigan, New Jersey y Florida (EUA) registraron un gran número de descomposturas. Se reportaron casos de boletas erróneas presentadas, muchas urnas electrónicas presentaron demoras demasiado largas, causando que muchos votantes desistieran. En algunos casos, las autoridades electorales pidieron a los votantes hacerlo en papel, sin que esto fuera en papelería electoral provista centralmente. (Gordon 2008)

Fuente Periodístico

Etiquetas Negación de servicio, integridad

Figura 4.22: Caso 7 evaluado bajo 7RP

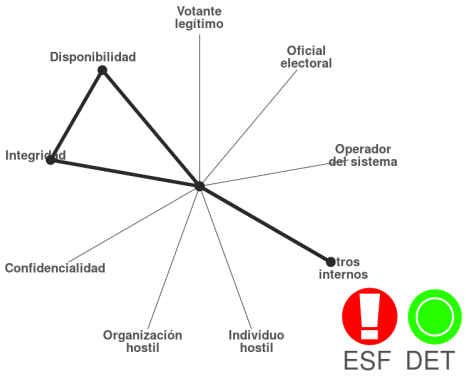


Figura 4.23: Caso 7 evaluado bajo AAVSU

Figura 4.24: Caso 7 evaluado bajo RODC

4.3.8. Israel, 2008

Las elecciones primarias del Partido Laborista en Israel tuvieron que suspenderse y posponerse cuando la jornada electoral estaba ya en marcha. Numerosos equipos presentaban problemas de usabilidad, como pantallas que no respondían al tacto, registraban votos sin ser tocadas, o registraban opciones distintas a las elegidas. La elección completa se canceló y celebró un día más tarde en papel. (Khoury, Singer-Heruti e Ilani 2008)

Fuente Periodístico

Etiquetas Usabilidad, calibración, negación de servicio, auto-votos

Figura 4.25: Caso 8 evaluado bajo 7RP

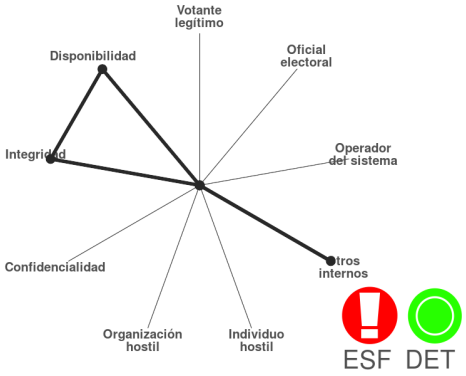


Figura 4.26: Caso 8 evaluado bajo AAVSU

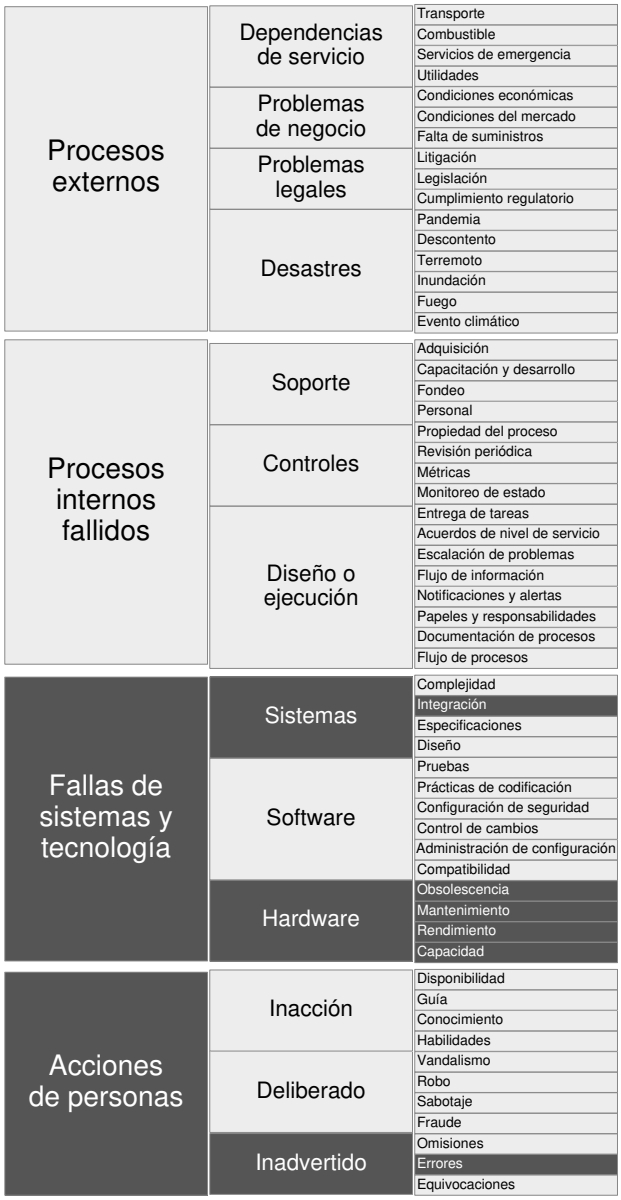


Figura 4.27: Caso 8 evaluado bajo ROdC

4.3.9. Holanda, 2008

Después de que un grupo de activistas demostró en TV en vivo cómo modificar la programación de las urnas *Nedap*, la Comisión Asesora en Procesos Electorales determina, ante la imposibilidad de asegurar la corrección de los fallos, volver de forma definitiva al voto en papel. (Election Process Advisory Commission 2007; WijVertrouwenStemComputersniet.nl 2009)

Fuente Reporte

Etiquetas Demostración, reprogramación, decisión legal

Figura 4.28: Caso 9 evaluado bajo 7RP

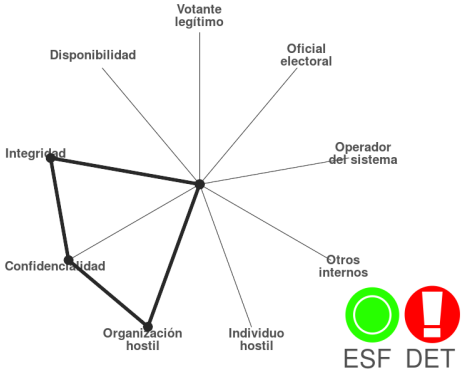


Figura 4.29: Caso 9 evaluado bajo AAVSU

Figura 4.30: Caso 9 evaluado bajo ROdC

4.3.10. Brasil, 2009

El Tribunal Superior Electoral de Brasil lanzó una convocatoria pública para encontrar fallos en sus urnas electrónicas. Sergio Freitas da Silva logra monitorear remotamente el voto conforme lo van emitiendo los ciudadanos por emisiones radiomagnéticas (rompiendo el principio de secrecía) empleando únicamente equipo casero con costo de algunas decenas de dólares. (Tribunal Superior Eleitoral, Brasil 2009; Felitti 2009; Busaniche 2009)

Fuente Auditoría

Etiquetas Radiofrecuencia, secrecía, convocatoria

Figura 4.31: Caso 10 evaluado bajo 7RP

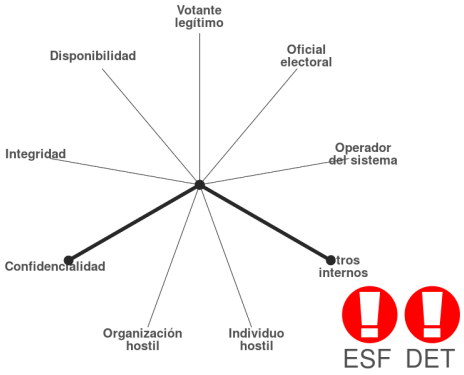


Figura 4.32: Caso 10 evaluado bajo AAVSU

Figura 4.33: Caso 10 evaluado bajo ROdC

4.3.11. India, 2010

La India tiene la implementación más grande existente de voto electrónico. Tres investigadores lograron alterar el resultado emitido por una urna EVM en pocos minutos, atacando el despliegue de resultados (no la captura o almacenamiento) (Prasad y col. 2010)

Fuente Adversarial

Etiquetas Ataque, despliegue, modificación, integridad

Figura 4.34: Caso 11 evaluado bajo 7RP

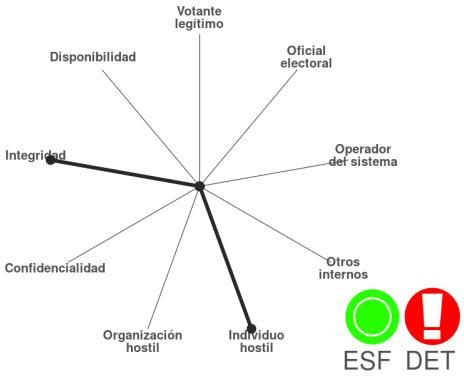


Figura 4.35: Caso 11 evaluado bajo AAVSU

Figura 4.36: Caso 11 evaluado bajo ROdC

4.3.12. Washington DC, EUA, 2010

La ciudad de Washington D.C. desarrolló un sistema para implementar voto en línea para sus ciudadanos residentes en el extranjero, y lo corrieron en un piloto para probar su seguridad. Un equipo lidereado por el investigador Alex Halderman encontró, en menos de 48 horas, una cadena de fallos que les permitieron, a partir de enviar una boleta con un nombre de archivo *trucado*, obtener control pleno de los servidores, incluyendo reemplazar votos ya emitidos por mal manejo del material criptográfico y comprometer la secrecía de los votos emitidos a partir de la intrusión. (Wolchock y col. 2012)

Fuente Auditoría

Etiquetas Remoto, vulnerabilidad, voto en línea

Figura 4.37: Caso 12 evaluado bajo 7RP

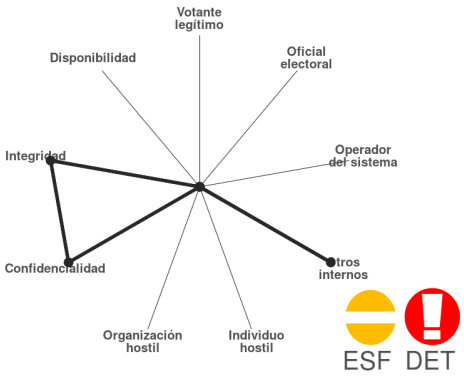


Figura 4.38: Caso 12 evaluado bajo AAVSU

Figura 4.39: Caso 12 evaluado bajo ROdC

4.3.13. Israel, 2010

Los investigadores Yossef Oren y Avishai Wool documentan cómo puede establecerse un ataque de *relay* sobre las boletas-RFID extendiendo el rango desde el cual éstas pueden ser consultadas (nominalmente 5 cm), permitiendo averiguar el sentido de los votos conforme son emitidos, modificar los votos emitidos, causar negaciones de servicio, y hasta eliminar los datos de una casilla completa. (Oren y Wool 2010)

Fuente Adversarial

Etiquetas RFID, integridad, negación de servicio

Figura 4.40: Caso 13 evaluado bajo 7RP

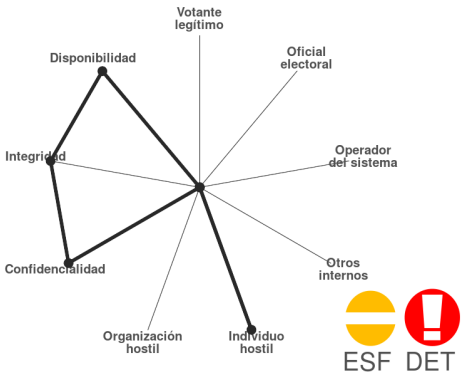


Figura 4.41: Caso 13 evaluado bajo AAVSU

Figura 4.42: Caso 13 evaluado bajo ROdC

4.3.14. Rio de Janeiro, Brasil, 2012

Un atacante de 19 años, Alexandre Neto, relata cómo interceptó, retardó y modificó los resultados de la elección para alcalde de la Región de los Lagos, Estado de Rio de Janeiro, Brasil, indicando incluso con nombre y apellido quién fue el beneficiado de dicha acción. (Gomes 2012)

Fuente Periodístico

Etiquetas Retraso, alteración, fraude, integridad

Figura 4.43: Caso 14 evaluado bajo 7RP

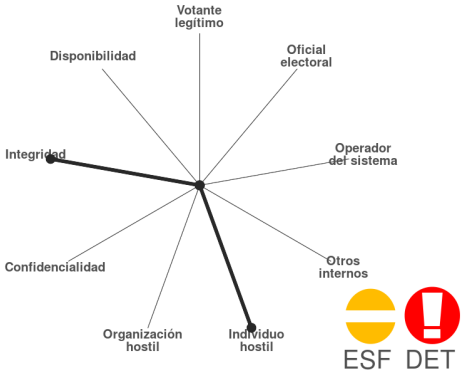


Figura 4.44: Caso 14 evaluado bajo AAVSU

Figura 4.45: Caso 14 evaluado bajo ROdC

4.3.15. Jalisco, México, 2012

El Instituto Electoral y de Participación Ciudadana de Jalisco (IEPC), México, efectuó un piloto productivo en la votación presidencial de 2012: La región de Los Altos de Jalisco votó mediante urnas electrónicas. Previo a este piloto, se hicieron cinco *simulacros* para lograr la familiarización de la población con esta modalidad. Las urnas diseñadas para esta elección contemplan el envío de las actas a la sede del IEPC por vía de telefonía celular al terminar la jornada electoral. Una de las quejas más comunes que se presentaron durante los simulacros es que, por la orografía y pobreza de la región, no hay cobertura celular en buena parte de los municipios que participaron de la prueba. En dichos casos, los resultados se obtuvieron de las urnas, y se transmitieron en papel. (El Informador 2012)

Fuente Periodístico

Etiquetas Telecomunicaciones, detección de requisitos

Figura 4.46: Caso 15 evaluado bajo 7RP

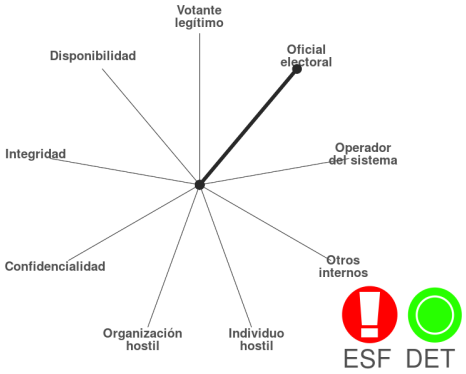


Figura 4.47: Caso 15 evaluado bajo AAVSU

Figura 4.48: Caso 15 evaluado bajo ROdC

4.3.16. Francia, 2013

El partido *Les Republicans* celebró sus elecciones primarias mediante voto por Internet. Un grupo de periodistas divulgó que el sistema permitía efectuar múltiples votos sin verificar la identidad; el candidato François Fillon (derrotado por poco) reclamó "fraude a escala industrial". (Lichfield 2013)

Fuente Periodístico

Etiquetas Fraude, en línea, unicidad, autenticación

Figura 4.49: Caso 16 evaluado bajo 7RP

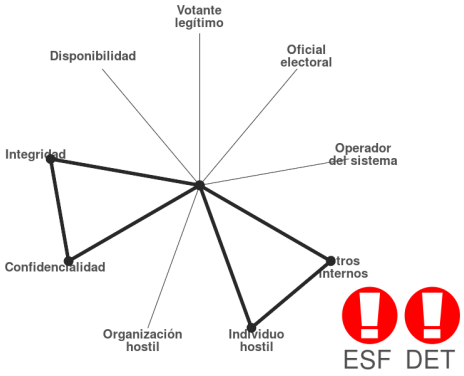


Figura 4.50: Caso 16 evaluado bajo AAVSU

Figura 4.51: Caso 16 evaluado bajo ROdC

4.3.17. Azerbaijan, 2013

La Comisión Central Electoral de Azerbaijan desarrolló una aplicación para dispositivos móviles para dar a conocer con oportunidad los resultados de la elección presidencial. Varios votantes reportaron que la aplicación comenzó a anunciar los porcentajes de votación obtenida, llevando a la reelección del presidente Aliyev, 12 horas antes de que la elección iniciara. (Ray 2013)

Fuente Periodístico

Etiquetas Fraude, pre-llenado, móviles

Figura 4.52: Caso 17 evaluado bajo 7RP

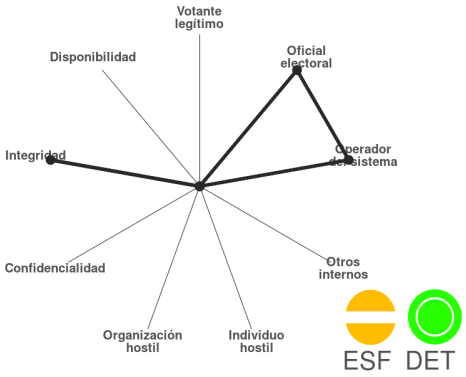


Figura 4.53: Caso 17 evaluado bajo AAVSU

Figura 4.54: Caso 17 evaluado bajo ROdC

4.3.18. Brasil, 2013

El Tribunal Supremo Electoral brasileño convocó, tras casi dos décadas de uso, a una auditoría limitada a las urnas electrónicas DRE que operan en Brasil. Un grupo de investigadores demostraron, tras únicamente una hora para familiarizarse con su código fuente (Aranha y col. 2013):

- La ruptura del mecanismo que busca asegurar la secrecía del voto
- Uso incorrecto de cifrado que hace vulnerables las llaves privadas
- Suposiciones erróneas al plantear el modelo de ataque
- Insuficiente auto-verificación del sistema

Fuente Auditoría

Etiquetas Secreto, integridad, ataques internos, modelo de ataque

Figura 4.55: Caso 18 evaluado bajo 7RP

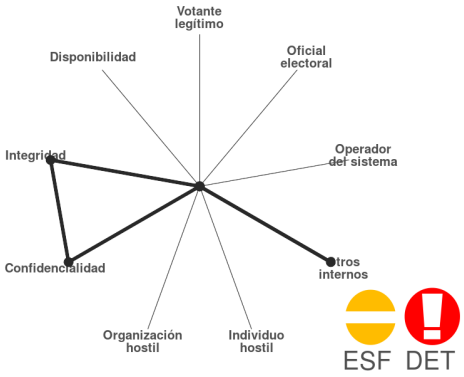


Figura 4.56: Caso 18 evaluado bajo AAVSU

Figura 4.57: Caso 18 evaluado bajo RODC

4.3.19. Estonia, 2014

El pequeño país báltico de Estonia se ha presentado como ejemplo y caso de éxito en la implementación de voto por Internet para la totalidad de su población. Springall y col. 2014 presentan dos ataques de lado de cliente, que permiten burlar la verificación vía celular o vía la tarjeta de ID nacional, y demuestran ataques de lado de servidor que evidencian que el modelo de atacante de las autoridades es incompleto

Fuente Adversarial

Etiquetas Integridad, modelo de ataque

Figura 4.58: Caso 19 evaluado bajo 7RP

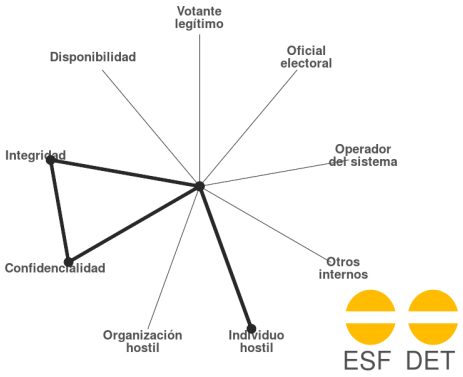


Figura 4.59: Caso 19 evaluado bajo AAVSU

Figura 4.60: Caso 19 evaluado bajo ROdC

4.3.20. Argentina, 2015

El sistema hoy conocido como *boleta electrónica* inició su implementación en Argentina en la provincia de Salta (noroeste). Para el 2015, la Ciudad Autónoma de Buenos Aires lo adoptó oficialmente, buscando cumplir con una legislación que detalla el tipo de equipo que es legal emplear (Ciudad Autónoma de Buenos Aires 2014, Anexo I, artículo 24, párrafo p). El investigador Javier Smaldone documenta que los equipos empleados contravienen el marco legal dentro del cual fueron adquiridas y no únicamente llevan una computadora oculta, sino que ésta tiene expuesta al exterior la interfaz de depuración JTAG, que permite la manipulación de la memoria no volátil del dispositivo. (Smaldone 2015)

Fuente Adversarial

Etiquetas Verificación, especificaciones, integridad

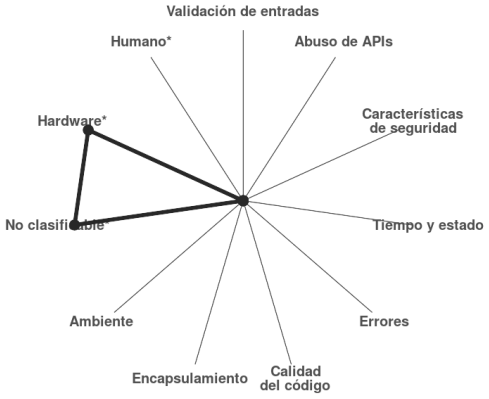


Figura 4.61: Caso 20 evaluado bajo 7RP

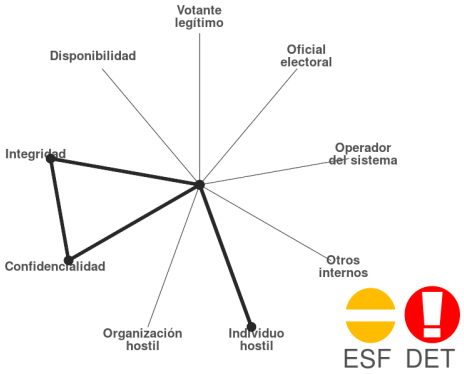


Figura 4.62: Caso 20 evaluado bajo AAVSU

Figura 4.63: Caso 20 evaluado bajo ROdC

4.3.21. Argentina, 2015

Un equipo de investigadores se enfocó en el equipo de boleta electrónica descrito en la sección 4.3.20. Entre muchos fallos "menores", como un uso inseguro de verificación por hashes criptográficos MD5 no firmados, encontraron que el chip RFID que guardan las boletas de dicho sistema son vulnerables a un ataque multivoto: Una misma boleta puede almacenar múltiples votos. (Amato y col. 2015)

Fuente Adversarial

Etiquetas RFID, Fraude, integridad, falta de verificación

Figura 4.64: Caso 21 evaluado bajo 7RP

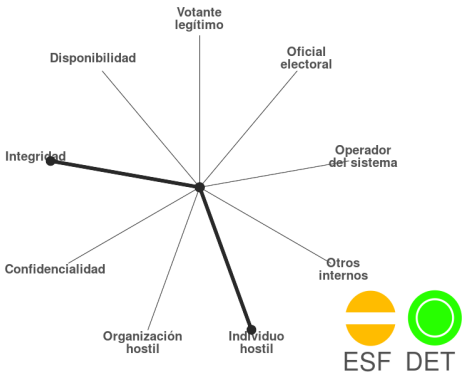


Figura 4.65: Caso 21 evaluado bajo AAVSU

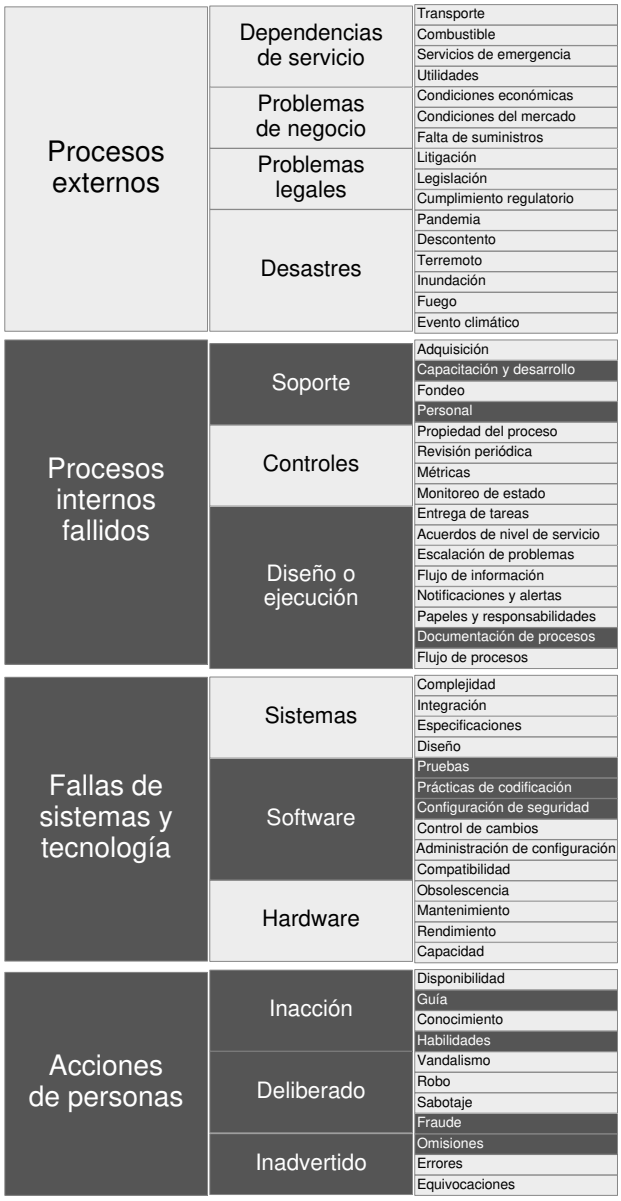


Figura 4.66: Caso 21 evaluado bajo ROdC

4.3.22. Bulgaria, 2015

En octubre de 2015 se presentó a referendo, en Bulgaria, la posibilidad de implementar voto electrónico a distancia. El mismo día, la Comisión Electoral Central fue blanco de un ataque de negación de servicio distribuido (DDoS). Si bien los reportes indican que el ataque fue contrarrestado a tiempo (y el referendo se realizó en papel), el ataque apunta a levantar dudas acerca de la factibilidad del voto sobre Internet, constituyendo una suerte de propaganda negativa en un momento que debería respetarse la veda de publicidad electoral. (Xinhua 2015)

Fuente Periodístico

Etiquetas Disponibilidad, en línea, negación de servicio

Figura 4.67: Caso 22 evaluado bajo 7RP

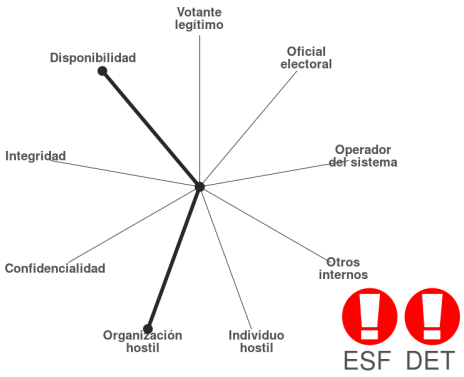


Figura 4.68: Caso 22 evaluado bajo AAVSU

Figura 4.69: Caso 22 evaluado bajo ROdC

4.3.23. Distrito Federal, México, 2015

El Distrito Federal celebra votaciones de presupuesto participativo, y para la elección de 2015 se permitió a los votantes sufragar en papel o sobre Internet, dado un pre-registro para esta segunda opción. Se presentaron acusaciones de fraude, ante acusaciones de altas ilegítimas para voto en línea, y de patrones sospechosos de participación por modalidad. (Bolaños Sánchez 2015)

Fuente Periodístico

Etiquetas Fraude, voto en línea, autenticación

Figura 4.70: Caso 23 evaluado bajo 7RP

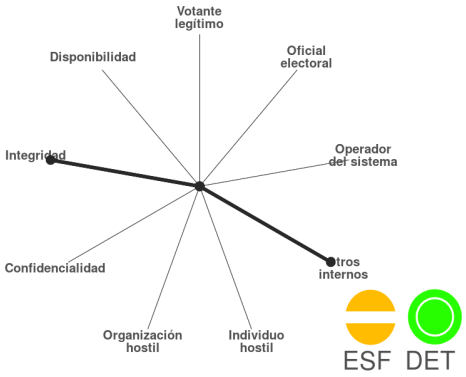


Figura 4.71: Caso 23 evaluado bajo AAVSU

Figura 4.72: Caso 23 evaluado bajo ROdC

4.3.24. Chiapas, México, 2015

Personal de la empresa contratada para el patrón del voto en línea desde el extranjero inscribió a residentes chiapanecos como si fueran residentes en el extranjero, con lo que se les impidió votar presencialmente; aparecieron como habiendo emitido sufragio en línea. (Henríquez 2015)

Fuente Periodístico

Etiquetas Padrón, fraude, voto en línea

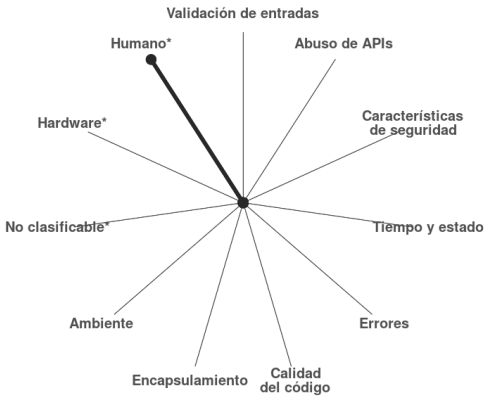


Figura 4.73: Caso 24 evaluado bajo 7RP

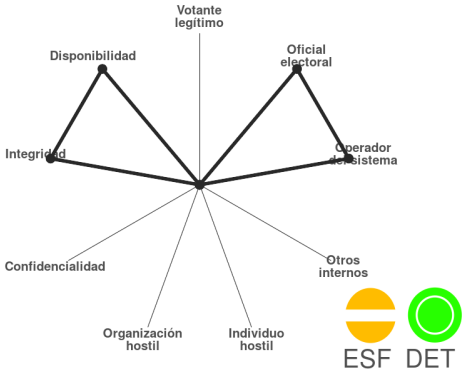


Figura 4.74: Caso 24 evaluado bajo AAVSU

Figura 4.75: Caso 24 evaluado bajo ROdC

Capítulo 5

Resultados

El presente capítulo reporta los resultados obtenidos del trabajo detallado en la Sección 4. La Sección 5.1 revisa lo que se puede observar del etiquetado temático abierto empleado como primer acercamiento; las Secciones 5.2, 5.3 y 5.4 presentan, respectivamente, a las taxonomías 7RP, ROdC y AASVU; finalmente, la Sección 5.5 evalúa la aplicabilidad de los distintos modelos de madurez observados al conjunto de datos sobre el cual se realizó el presente trabajo.

Antes de entrar en materia, conviene recordar al lector que las fuentes de datos disponibles para los artículos presentados son de naturaleza muy distinta: La cantidad y profundidad de la información disponible de un artículo académico no puede compararse con lo que se puede aprender de una nota periodística; La gráfica 5.1 presenta el número de casos provenientes de cada tipo de fuente, mismos que se abordan a continuación:

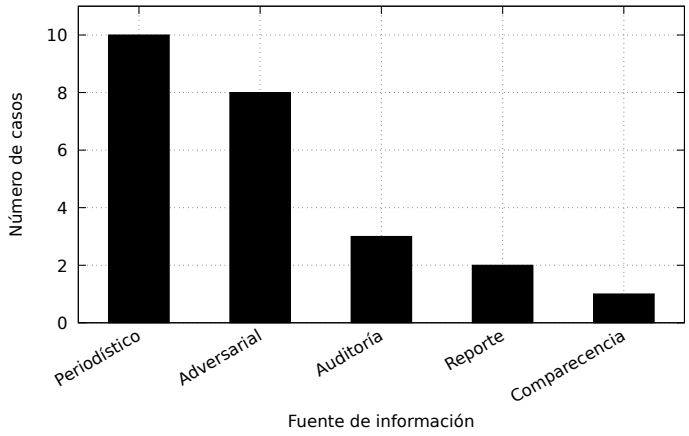


Figura 5.1: Número de casos provenientes de los diferentes tipos de fuentes de información identificados.

Periodístico La principal fuente de datos es el recuento que algún medio noticioso hace respecto al incidente. Es de estos casos que menos es posible reportar, dado que si bien estos medios hacen un relato fáctico de lo ocurrido, al no profundizar en los detalles, las causas y consecuencias, obligan a que la evaluación realizada resulte muy somera.

Adversarial Los casos derivados de la publicación de detalles de ataques a aspectos específicos del voto

electrónico desarrollados por personas o equipos *ajenos* a la autoridad electoral actuando *sin su autorización* se etiquetan como *adversariales*. Para estos casos, si bien típicamente se presentan reportes detallados que explican lo suficiente la debilidad que explotan, pocas veces incluyen información organizacional relevante de la autoridad electoral que pueda llevar a explicar el *por qué* de la elección tecnológica, configuración o proceso fallido en cuestión.

Auditoría Es tristemente muy raro que, ya sea autoridades electorales, ya sea proveedores particulares de equipo de voto electrónico, convoquen a auditorías públicas que lleven a que expertos busquen y reporten los fallos en sus sistemas. Al presentar los resultados de una auditoría podría revelarse información fundamental que lleve a una completa comprensión de un fallo, sus causas y consecuencias. De los casos reportados, únicamente tres pueden clasificarse de esta manera. Cabe mencionar que los tres consisten en ejercicios limitados; las condiciones impuestas por la autoridad para la celebración de dichas auditorías resultan mucho más limitadas que el ataque que podría realizar un atacante malicioso — Pero es lo más que se ha logrado.

Reporte Dos casos de fallos en la implementación de esquemas de voto electrónico presentaron resultados tan contundentes que han llevado a la autoridad electoral a hacer un estudio detallado y minucioso al respecto, que han tenido por consecuencia la publicación un documento formal y completo de análisis *post-mortem*. Son documentos formales, detallados, y abordan detalles de los procesos internos de la autoridad electoral, brindando información completa respecto a cada uno de los pasos relevantes. En ambos casos, la conclusión de la autoridad electoral fue abandonar la adopción de esquemas de voto electrónico.

Ambos casos fueron motivados por información originalmente de menor profundidad (en el primer caso, periodística; en el segundo, adversarial).

Comparecencia Hay un único caso que entra en este supuesto: La audiencia pública en que un desarrollador de sistemas afirma haber estado involucrado en el desarrollo de un sistema de voto electrónico con la indicación expresa de hacerlo con la capacidad de permitir el robo de votos.

5.1. Etiquetado simple

En el ejercicio de etiquetado simple fueron identificados 45 términos únicos; a lo largo de los 24 casos, ninguno tiene únicamente una etiqueta, seis tienen dos, 12 tienen tres, y seis tienen cuatro, promediando 3 etiquetas por caso.

Se elaboró un concentrado de la frecuencia de la ocurrencia de los términos del etiquetado, ordenados de forma descendente; la Gráfica 5.2 presenta a aquellas que fueron empleadas en más de una ocasión:

10 veces Integridad

7 veces Fraude

4 veces Negación de servicio

3 veces Voto en línea

2 veces Autenticación, Diebold, En línea, Padrón, RFID, Usabilidad, Verificación, Modelo de ataque

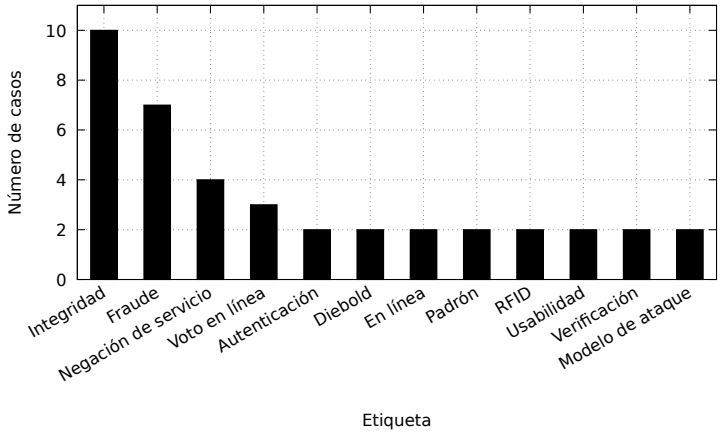


Figura 5.2: Etiquetas que fueron empleadas en más de una ocasión para describir el conjunto de datos estudiado

1 vez Alteración, Ataque, Ataques internos, Auto-votos, Calibración, Concordancia, Confesión, Convocatoria, Código fuente, Decisión legal, Demostración, Despliegue, Detección de requisitos, Discrepancia, Disponibilidad, Error aritmético, Especificaciones, Falsa seguridad, Falta de verificación, Modificación, Móviles, Plan de contingencia, Pre-llenado, Radiofrecuencia, Remoto, Reprogramación, Resguardo, Retraso, Secrecía, Secreto, Telecomunicaciones, Unicidad, Vulnerabilidad

El etiquetado simple, sin embargo, no puede ser considerado para hacer un análisis objetivo, principalmente por su falta de universalidad — Consiste en una serie de términos que el catalogador les asigna arbitrariamente en el momento, razón por la cual carece de repetibilidad, y puede ser únicamente aceptado como un descriptor genérico de cada caso, ayudando al lector a encontrar a simple golpe de vista los aspectos en que el catalogador reparó.

5.2. Evaluación sobre 7RP

La taxonomía presentada en la Sección 2.4.1, *Siete Reinos Perniciosos* (Tsipenyuk, Chess y McGraw 2005; Tsipenyuk, Chess y McGraw 2006), está enfocada completamente al proceso de *desarrollo de software*. Como puede apreciarse en la Figura 5.3, y como ya se adelantó, nuestro análisis mostró que requerían agregarse tres columnas: *No clasificable*, *Hardware* y *Humano*.

Esto se hizo dado que, como puede apreciarse en la Figura 5.4, dichas columnas representan las causas más prevalentes de los problemas observados. Si la clasificación se hubiera realizado estrictamente sobre las 7+1 categorías originalmente definidas para esta taxonomía,[1] once de los casos caerían completamente fuera del dominio; fue únicamente agregando estas tres categorías que se da cobertura significativa a la muestra. La Figura 5.3 muestra el origen de cada una de las categorías referidas; salta a la vista que, de no haberse agregado las categorías adicionales, se terminaría omitiendo de parte importante de la muestra.

La taxonomía en cuestión se enfoca exclusivamente al proceso de desarrollo de software; los factores relacionados con problemas en el hardware, o del factor humano (que es parte inseparable del *sistema electoral*) escapan a su ámbito.

[1] El documento que presenta 7RP presenta al *ambiente*, elementos ajenos al código fuente pero críticos para su despliegue, como un *octavo reino*, sin que esto afecte al nombre que se da a la taxonomía toda.

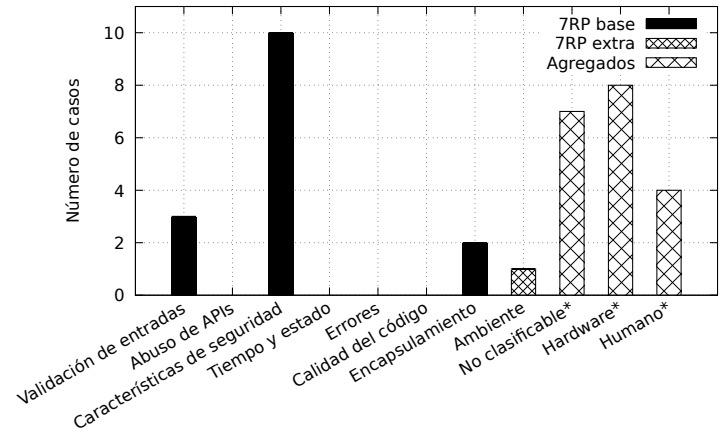


Figura 5.3: Número de casos por categoría primaria de 7RP

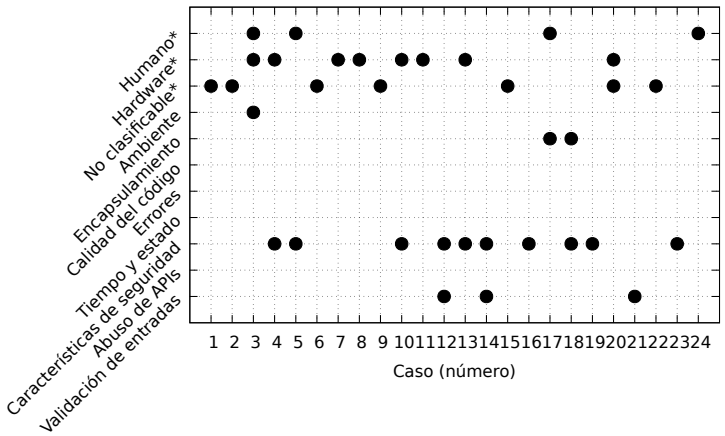


Figura 5.4: Clasificación por caso por categoría primaria de 7RP

Esto no debe tomarse como una crítica a 7RP, una taxonomía ampliamente respetada y aceptada, sino su aplicabilidad *a los problemas observados*. Cabe enfatizar en la fuente de información presentada en la Sección 4 — Estos casos se obtuvieron y clasificaron a partir de la información periodística disponible; no se tiene acceso en la mayor parte de los casos a información técnica completa respecto a cada uno de ellos, por lo que –incluso en el caso de deberse un fallo al proceso de desarrollo de software– no se cuenta con el detalle de información requerido.

5.3. Evaluación sobre *Riesgos Operacionales de Ciberseguridad*

La segunda taxonomía que aborda el presente trabajo, presentada en la Sección 2.4.2 (Cebula, Popeck y Young 2014) cubre el dominio problematizado mucho mejor. Como puede apreciarse en la Figura 5.5, la cobertura del universo presentado por esta taxonomía es mucho más homogéneo que en el caso de 7RP: No hay una concentración tan desmedida como la vista en el caso anterior sobre un sólo vector, y no hay espacios tan amplios que no registren caso alguno.

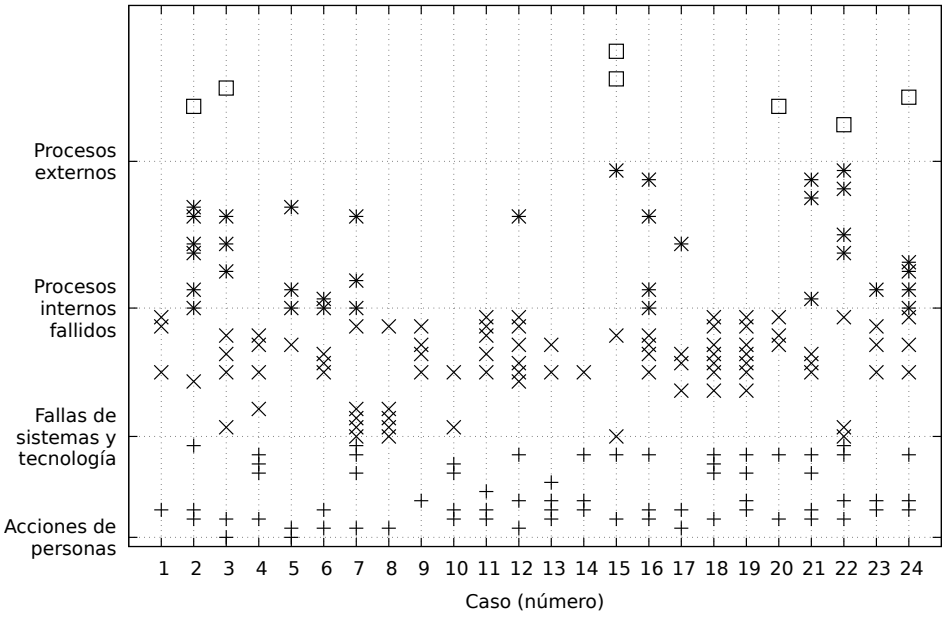


Figura 5.5: Casos por categoría de ROdC, a su máxima granularidad (57 categorías); las etiquetas sobre el eje vertical y el tipo de marca corresponden al primer nivel de la taxonomía

Ante un primer acercamiento, salta a la vista que la categoría de primer nivel *Procesos externos* presenta muy poca actividad, seguida de *Procesos internos fallidos*; la mayor parte de actividad se concentra en *Acciones de personas* y *Fallas de sistemas y tecnología*.

Totalizando los casos por categoría, como ilustra la Figura 5.6 puede apreciarse que sí hay algunas categorías preocupantemente populares. Las categorías que aparecen en un tercio de los casos (ocho menciones), de mayor a menor incidencia, así como su descripción (en traducción propia) en el documento de Cebula, Popeck y Young 2014, son:

16 Fallas de sistemas y tecnología → Software → Configuración de seguridad

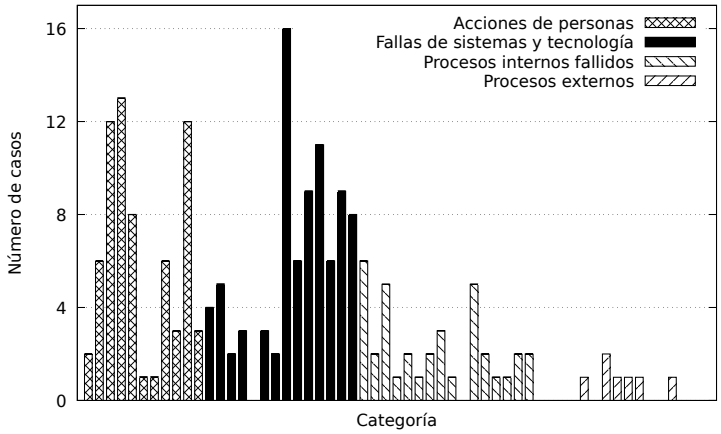


Figura 5.6: Número de casos por categoría de ROdC; el patrón de relleno corresponde al primer nivel de la taxonomía

Aplicación y administración incorrecta de configuraciones y parámetros apropiados para el uso esperado

13 Acciones de personas → Deliberado → Fraude

Acción deliberada tomada para beneficio propio o de un colaborador a expensas de la organización

12 Acciones de personas → Inacción → Guía

Un individuo con conocimiento sin la guía o dirección correcta para emprender acciones

12 Acciones de personas → Inadvertido → Omisiones

Individuo que no llevó a cabo una acción correcta conocida, frecuentemente por realizar un procedimiento apresuradamente

11 Fallas de sistemas y tecnología → Sistemas → Diseño

Falta de adecuación del sistema para su uso o aplicación esperado

9 Fallas de sistemas y tecnología → Sistemas → Integración

Falla en el funcionamiento conjunto o interfaz entre varios componentes del sistema; también incluye falta de pruebas

9 Fallas de sistemas y tecnología → Software → Pruebas

Pruebas inadecuadas o atípicas en la configuración o aplicación del software

8 Fallas de sistemas y tecnología → Sistemas → Complejidad

Sistema demasiado intrincado o un gran número de interrelaciones entre componentes

8 Acciones de personas → Deliberado → Sabotaje

Acción deliberada para causar una falla en un activo o proceso organizacional, generalmente efectuado contra activos llave específicos por alguien con acceso a conocimiento interno

El hecho de que dos terceras partes de los casos abordados hayan presentado fallos derivados (al menos parcialmente) de su configuración de seguridad resulta a todas luces alarmante. La mitad o más casos fueron

Número de casos por categoría de primer nivel según RODC

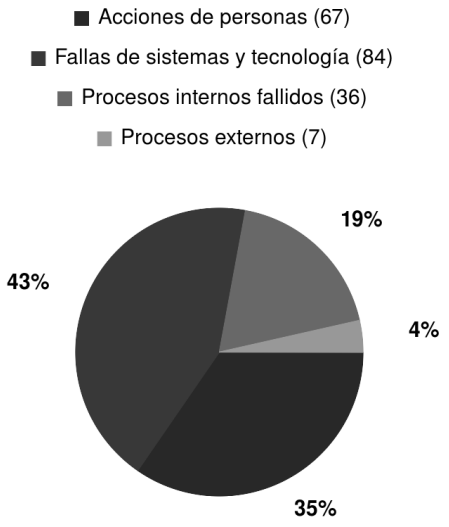


Figura 5.7: Suma de todas las ocurrencias dentro de cada caso

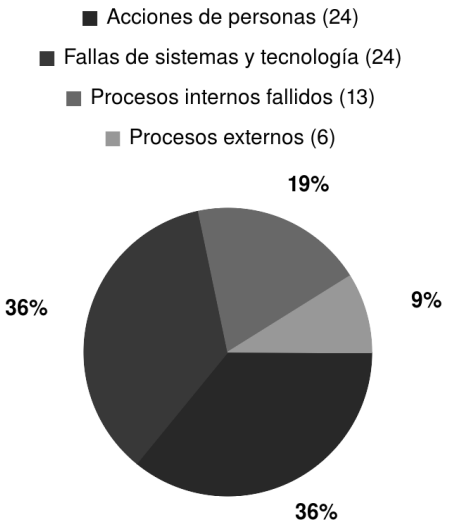


Figura 5.8: Limitando a una ocurrencia por categoría de primer nivel por caso

catalogados como fraude, falta de guía y omisión. Esto es, la gran mayoría de los problemas presentados se debió a la *impericia, incompetencia o falta de lealtad* de los participantes implicados. Cabe mencionar que esto contrasta con los reportes de tendencias globales, en que únicamente el 20 % de pérdidas[2] por incidentes de seguridad se deben a atacantes internos (Richardson 2008, p.14).

Por otro lado, si se considera únicamente el nivel más externo de la taxonomía, se encuentra la situación que se observa en las Figuras 5.7 y Figura 5.8; la primera no presenta ninguna sorpresa fundamental respecto a la información ya presentada en la Figura 5.6, pero la Figura 5.8 presenta un nuevo hecho alarmante: Tanto la primera como la segunda categorías, *Acciones de personas* y *Fallas de sistemas y tecnología*, estuvieron presentes en *la totalidad* de los casos abordados. Una pequeña mayoría de casos (13 de 24) entró en la clasificación de *Procesos internos fallidos*, en tanto la proporción de *Procesos externos*, si bien no resulta insignificante, queda claramente rezagada.

En suma, de la taxonomía RODC emerge la necesidad de enfatizar en atender a los fallos en sistemas y tecnología (sea en sistemas, software o hardware) muchas veces derivados de los fallos de las personas, ya sea deliberados, inadvertidos o por inacción. Resulta pertinente apuntar que una correcta aplicación de modelos de madurez específicos al dominio problematizado (ver las Secciones 2.5 y 5.5) podría ser importante para prevenir fallos como los aquí abordados; su diseño, como fue ya expuesto desde las Secciones 1.4 y 1.5, resulta una tarea que excede con mucho el ámbito del presente trabajo, y requiere involucramiento de expertos de forma transdisciplinaria.

[2]El reporte citado explicita que esta cifra se refiere a pérdidas económicas, lo cual no es directamente trasladable a un dominio como el que aquí se estudia; el punto mencionado, sin embargo, es ilustrativo a la proporción de riesgos en el mercado.

5.4. Evaluación sobre *Análisis de Amenazas en Sistemas de Votación UOCAVA*

Por último, se presenta la evaluación resultante del análisis de nuestro conjunto de datos mediante la taxonomía desarrollada por Regenscheid y Hastings 2008 (presentada en la Sección 2.4.3).

En primer término, la aplicación de esta taxonomía resulta menos clara que la de las dos previamente abordadas; esto se debe en parte a la poca información que hay disponible dado el origen periodístico de la mayor parte de las notas, como se indicó al presentar los casos en la Sección 4, pero también porque el modelo de riesgos que contempla no es explícito en su aplicación.

Para ilustrar el punto, una de las principales categorías que presenta AASVU es la fuente de la amenaza. La taxonomía presenta cuatro fuentes internas (votantes legítimos; oficiales electorales; operadores del sistema; otros internos) y dos externas (individuos hostiles; organizaciones hostiles). Ahora bien, como es común en el campo de la seguridad informática, existe una enorme diferencia entre *quién puede hacerlo la primera vez* y *quién puede hacerlo en ocasiones subsecuentes*. Piénsese, como símil, en el impacto de una vulnerabilidad *0-day*[3] comparada con el que tendría una vez que los desarrolladores son notificados y transcurrió suficiente tiempo para la publicación de la corrección el alertamiento de los usuarios.

Tomando como ejemplo, entonces, al caso en que Ed Felten descubre que las urnas *AccuVote-TS* pueden ser abiertas con una llave genérica empleada para archiveros, minibares y *rockolas* (véase la Sección 4.3.4): Dado que se trata de una vulnerabilidad publicada, no de un ataque realizado, ¿debería clasificarse según el conocimiento público al momento de su descubrimiento (en que sólo el profesor Felten sabía del fallo), o se debe considerar el impacto posterior (con el cual es conocimiento público)? En el primer caso, sólo se marca *individuo hostil*, en el segundo caso, cualquiera de los actores puede llevarlo a cabo. Para este trabajo, se tomó la primera alternativa, dado que se aborda al incidente en el momento de su aparición, pero a sabiendas de que el desarrollo en el campo no ocurre *en el vacío*: Debe asumirse que los potenciales atacantes de hoy están al tanto de los desarrollos en el campo.

En los (desafortunadamente[4] pocos) casos en que un fallo es descubierto gracias a una convocatoria a verificación o auditoría, el origen del ataque se considera como *otro interno*, no como un *individuo hostil*.

Esta decisión, sin embargo, crea una distorsión en los resultados: La categoría de *otro interno* resulta demasiado amplia. Citando a Regenscheid y Hastings 2008, esta corresponde a (traducción propia):

> Otros individuos u organizaciones que pueden tener acceso privilegiado al equipo de votación, ya sea antes, durante o después de realizada una elección. Por ejemplo:
>
> - Fabricantes de sistemas de votación
> - Integradores de sistemas de votación
> - Personal de soporte

Las Figuras 5.9 y 5.10 presentan el resumen cuantitativo de la aplicación de AASVU a los casos estudiados. Puede apreciarse que:

- El actor causante de los incidentes abordados se debieron en 11 ocasiones a *otros internos*, lo cual no es de sorprender dada la explicación anterior; en nueve, a *individuos hostiles*; en cinco, a *oficiales*

[3] En la comunidad de la seguridad informática, se denomina de esta manera a una vulnerabilidad que no ha sido divulgada a los desarrolladores o usuarios de determinado sistema; no existe aún una solución o medidas propuestas de mitigación, y los atacantes que la conozcan pueden emplearla con alta probabilidad éxito para vulnerar a sus sistemas objetivo.

[4] La práctica de auditorías abiertas por expertos externos debería ser la regla, y no la excepción.

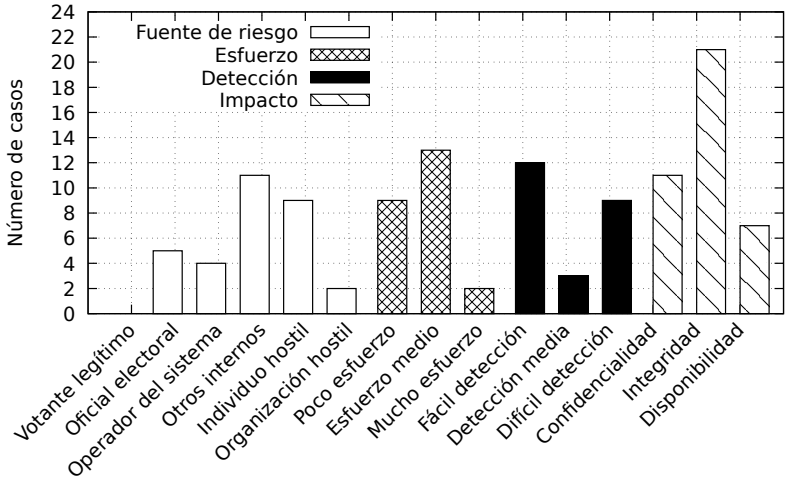


Figura 5.9: Número de casos por categoría dentro de la clasificación AAVSU; el patrón de relleno corresponde al primer nivel de la taxonomía.

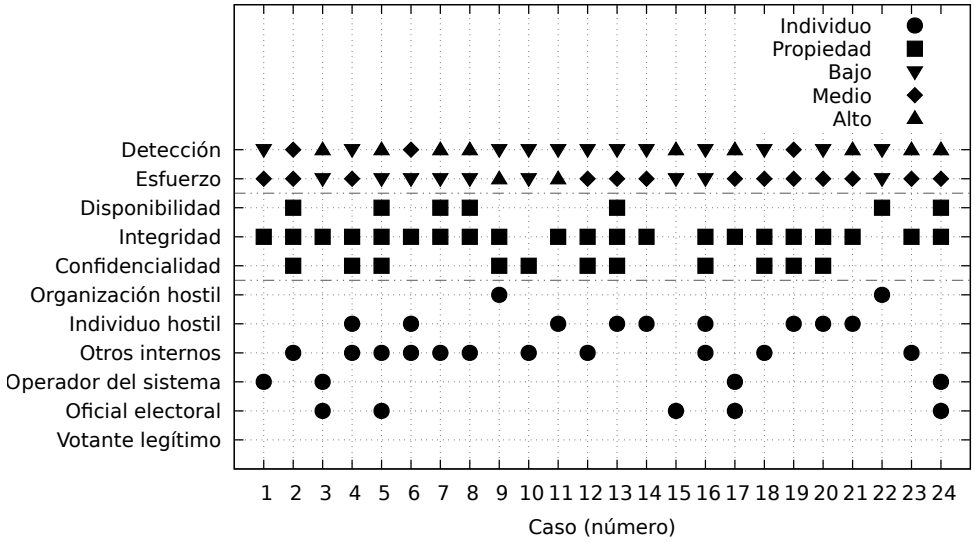


Figura 5.10: Casos por categoría de AASVU; la región inferior presenta las categorías relacionadas con la *fuente de riesgo*, la intermedia al tipo de *impacto*, y la superior, severidad del riesgo para esfuerzo requerido para un ataque y la dificultad de detección.

electorales; en cuatro, a *operadores del sistema*; en dos, a *organizaciones hostiles*. Los *votantes legítimos* no fueron causantes de ninguno de los casos presentados.

- El impacto de una abrumadora mayoría de los incidentes (21 de 24) está relacionado con la integridad; en 11 casos se refiere a la confidencialidad, y en siete a la disponibilidad.
  - Esto es perfectamente esperable: La principal amenaza a un sistema electoral es la integridad de la información; las demás propiedades son frecuentemente vistas como importantes pero supeditadas a ésta.
  - Llama la atención el caso 15 (véase la Sección 4.3.15), dado que es el único en que no se marcó ninguna de las propiedades. Esto se debe a que no se trata de un ataque, sino que un caso donde la realidad del terreno donde se desplegaron las urnas electrónicas no estaba contemplado en sus especificaciones técnicas: Las urnas contemplan la transmisión de resultados mediante la red celular; al no estar ésta disponible, no se comprometen disponibilidad, integridad ni confidencialidad — Únicamente la oportunidad de la comunicación a la cabecera del distrito electoral.
  - Tres de los casos (ver las Secciones 4.3.2, 4.3.5 y 4.3.13) impactan en los tres vectores definidos por esta taxonomía.
- Nueve casos están clasificados indicando que requieren *bajo esfuerzo* (mayor severidad), 13 requieren *esfuerzo mediano*, y únicamente dos *alto esfuerzo*.
  - En la mayor parte de los incidentes requirieron de un conocimiento o involucramiento no trivial (pero tampoco a detalle) del sistema; únicamente dos casos (refiérase a las Secciones 4.3.9 y 4.3.17) requirieron de un mucho mayor conocimiento o compenetramiento con el sistema atacado.
  - Los nueve casos marcados como de *bajo esfuerzo* incluyen a los cinco (véase las Secciones 4.3.3, 4.3.5, 4.3.7, 4.3.8 y 4.3.15) donde lo observado fue la falla en el funcionamiento de los equipos: No requerir de un atacante para caer en una falla es, necesariamente, *bajo esfuerzo*.
- 12 de los casos son de *baja facilidad de detección* (difícil detección, mayor severidad), tres de *facilidad de detección mediana*, y nueve de *alta facilidad de detección*.
  - La mayor parte de los calificados como de *alta facilidad de detección* son también de *bajo esfuerzo* (presentados en las Secciones 4.3.3, 4.3.5, 4.3.7, 4.3.8, 4.3.15) — Esto es, son fallos obvios o casi obvios en la operación normal de los equipos. De los cuatro restantes, tres responden a denuncias de irregularidades sobre procesos electorales en producción (Secciones 4.3.17, 4.3.23, 4.3.24), y únicamente uno (4.3.21) busca demostrar el fallo para alertar a las autoridades.
  - Los casos más peligrosos serían aquellos con tanto baja facilidad de detección como bajo esfuerzo. Estos son los presentados en las Secciones 4.3.10, 4.3.16 y 4.3.22.

5.5. Evaluación de los modelos de madurez

El lector notará que, si bien se mencionaron los modelos de madurez en conjunto con las taxonomías que se desarrollaron para la parte medular de éste trabajo, los modelos de madurez no formaron parte de la misma.

A continuación, se presentan las observaciones respecto a cada uno de los modelos de madurez presentados en la Sección 2.5, así como la evaluación global de su aplicabilidad a los casos estudiados en la Sección 5.5.5.

5.5.1. BSIMM

En un primer momento nos pareció que este modelo conectaría particularmente bien con el trabajo desarrollado dado que está construido alrededor del mismo espacio de problema que la taxonomía 7RP; no es casualidad que el autor primario de BSIMM participó como autor en dicha taxonomía (McGraw, Migues y West 2015; Tsipenyuk, Chess y McGraw 2006). BSIMM está orientado a la evaluación de la calidad específica en *procesos de desarrollo de software*, razón por la cual no considera a muchas de las variables que representarían a la realidad externa, al entorno en que se instrumenta el voto electrónico. La lista de vectores que componen a la versión 6 de BSIMM tienen una gran similitud con las categorías abordadas por la taxonomía 7RP (ver Sección 5.2):

Si bien BSIMM presenta algunas categorías adicionales a las de 7RP, particularmente las relacionadas a pruebas de penetración, pruebas de seguridad y modelos de ataque, se estima natural que al analizar los casos abordados mediante este modelo de madurez, dada la concentración de casos clasificados como *Humano* y *Hardware* en 7RP, se caería en las mismas carencias que las presentadas en la Sección 5.2: El desarrollo de software es únicamente una de las fases de la ejecución de proyectos tan complejos como los abordados en los casos estudiados. Muy pocos de ellos pueden verse como derivados de un mal proceso de desarrollo de software, por lo cual tampoco se podría esperar que el modelo de madurez BSIMM ilustre de forma significativa respecto a nuestro conjunto de datos.

5.5.2. ISMM

El *Modelo de Madurez de Seguridad de la Información* presenta una escala con cinco valores posibles que expresa qué tan completo es el manejo de la seguridad informática: *Ningún cumplimiento*, *Cumplimiento inicial*, *Cumplimiento básico*, *Cumplimiento aceptable* y *Pleno cumplimiento*.

La evaluación del nivel actual de determinada organización, así como los puntos a atender para poder transitar a niveles de madurez superiores, se realiza mediante el llenado de cuatro formularios, uno por cada uno de los *indicadores núcleo*: Administración de la seguridad, administración de servicios, arquitectura empresarial y Gobernanza corporativa. Cubre puntos tanto técnicos (por ejemplo, instalación de sistemas de prevención de incidentes o seguridad perimetral) como de gestión organizacional (como la disposición a la auditoría, frecuencia de verificación del cumplimiento regulatorio).

Respecto a la aplicabilidad de ISMM al estudio aquí presentado, sin embargo, no resulta posible dado que, como se expuso al inicio del Capítulo 4, la mayor parte de información acerca de los casos abordados fueron artículos periodísticos; únicamente los casos descritos en las Secciones 4.3.3, 4.3.10, 4.3.12, 4.3.15 y 4.3.18 (aproximadamente el 20 %) fueron desarrollados con la autorización de la autoridad electoral relevante. Podría asumirse que las autoridades electorales detrás de los cinco casos referidos han logrado una mayor madurez que la mayor parte de las otras (en particular, únicamente estas satisfarían a los puntos 4.3, 4.6, 4.8 y 4.10 del modelo), pero hay muchos otros aspectos que CCSMM requiere y no son evaluables sin información mucho más profunda que la disponible públicamente.

Este modelo de madurez podría aplicarse de cierta manera de forma inversa: Descontando puntos por todos los puntos que, dado el incidente, resultan naturalmente débiles. Por ejemplo, para el caso presentado en la Sección 4.3.21, resulta claro que los sistemas vulnerables en cuestión no cumplen satisfactoriamente con los puntos:

- 1.2.5 (presencia de un sistema de detección de intrusos)
- 1.3.1.3 (robo de información)

- 1.3.1.4 (intrusión en sistemas informáticos)
- 1.3.1.5 (mal uso de computadoras por parte del usuario)
- 2.1.10 (si el rendimiento es considerado menos que satisfactorio, se establecen requisitos claros)
- 2.1.13 (están activos sistemas efectivos para garantizar la seguridad de la propiedad)
- 3.1.1 (los usuarios están involucrados en el análisis arquitectural)
- 3.1.8 (se cuenta con un sistema para proveer rastreabilidad en toda la organización)
- 3.2.2 (una nueva arquitectura en seguridad emerge como resultado de la actualización de las suposiciones y diseños para encarar a retos emergentes)
- 3.2.6 (la seguridad está interconstruida tanto en la fase de planeación como en la de diseño)
- 3.2.15 (se implementa seguridad de la información)
- 3.2.17 (se cuenta con implementación de protección de software, que incluye protección de memoria y código verificado)
- 3.2.19 (se realizan regularmente auditorías de sistema)
- 3.3.1 (la organización identifica y enfrenta continuamente asuntos de seguridad)
- 3.3.3 (los empleados están entrenados en seguridad y en detección de riesgos
- 3.3.4 (todos los niveles de la organización comprenden la importancia de la seguridad, por lo que ésta se vuelve su territorio)
- 4.1 La organización cumple con políticas de seguridad

Sin embargo, aunque esto aparenta ser una lista larga, carece de expresividad para denotar muchas de las características de un ataque como el abordado. Aplicar esta lista de chequeo a los demás casos sólo haría más patente que no es un cuestionario que se puede realizar con un conocimiento casual de la problemática.

5.5.3. CCSMM

Este modelo pone particular énfasis en la conciencia colectiva respecto a la seguridad en un ámbito socio-geográfico — En primer término, claro, qué tanto importan los posibles riesgos o modelos de ataque a los individuos y organizaciones en cuestión, y qué tanto comparten y planifican en conjunto ante ellos.

Si se busca relacionar este modelo con las taxonomías presentadas, tiene particular cercanía con ROdC; si bien excluye explícitamente al área de *procesos externos*, las cuatro dimensiones de CCSMM (*Conciencia*, *Compartición de información*, *Políticas* y *Planes*) apuntan a consecuencias de buena parte de las subcategorías de las tres áreas restantes.

Por otro lado, al presentar el modelo de amenazas a que CCSMM responde, se nota un ligero paralelismo con AASVU: El primer paso para realizar una evaluación sobre este modelo de madurez es la severidad de un riesgo; clasifica a los riesgos en *no estructurados* (causados por individuos con capacidades medianas, empleados enojados, etc.), *estructurados* (grupos de individuos persiguiendo objetivos particulares, donde entra más en juego una ganancia económica), y *altamente estructurados* (llevados a cabo por profesionales

multidisciplinarios con amplio acceso a recursos). En consonancia, parte importante del modelo propuesto por AAVSU es determinar el nivel de esfuerzo y de detectabilidad de un ataque, también en tres niveles, ubicando a cada caso sobre este mismo vector.

CCSMM define cinco niveles de madurez: *Inicial*, *Establecido*, *Auto-evaluado*, *Integrado* y *Vanguardia*. El modelo, sin embargo, no resulta aplicable para el conjunto de datos evaluado — Por razones descritas en el mismísimo modelo: El acceso a la información, y el ámbito del análisis.

Respecto al primer punto, es necesario reiterar sobre el punto expuesto en la sección anterior: Dado que la mayoría de estos casos provienen de artículos periodísticos, no se tiene la riqueza de información necesaria para hacer una evaluación significativa.

El segundo punto resulta más medular al modelo CCSMM, y va muy de la mano con el planteamiento de origen del presente trabajo: Una entidad electoral *ocurre* dentro de una sociedad, y no puede explicarse sin relacionarse con su entorno. Intentar analizar a la entidad electoral de forma aislada, sin considerar su relación con partidos políticos, otras ramas del gobierno, empresas con intereses económicos, incluso las características no corporativas del entorno social en que ocurre, llevaría a un análisis incompleto y sesgado; si bien se determinó que CCSMM resulta ampliamente relevante para evaluar la madurez necesaria para evaluar si una entidad electoral está en capacidad de operar o no exitosamente un sistema de voto electrónico, llevar a cabo el análisis excede ampliamente lo que puede obtenerse de unos cuantos artículos periodísticos.

5.5.4. ISCMM

Los autores de ISCMM no llegan a desarrollar una propuesta completa de modelo de madurez como lo hacen los otros abordados, pero tocan un punto muy importante que CCSMM asume, aunque sin explicitarlo: Cómo la cultura corporativa se construye a partir de las rutinas diarias y comportamiento implícito de cada uno de sus participantes. Y, partiendo del análisis de una organización, así como CCSMM apunta hacia arriba (agregando varias organizaciones para analizar la madurez de una comunidad), ISCMM apunta hacia abajo (analizando el nivel de comprensión y compromiso con la seguridad de la información en cada uno de los individuos que la conforman).

ISCMM no tiene desarrollados puntos claros de medición para indicar si una organización está en un nivel o en otro; no se presenta como un modelo de madurez desarrollado, sino que como un trabajo *encaminado* a lograrlo. A pesar de haber sido presentado en 2006, no fue posible encontrar una versión del modelo de madurez claramente presentada como tal.

Esta propuesta está construida sobre el *modelo de aprendizaje del aprendizaje consciente* (Gullander 1974); Thomson y von Solms presentan las cuatro etapas (incompetencia inconsciente, incompetencia consciente, competencia consciente y competencia inconsciente), así como las transiciones necesarias (sensibilización, entrenamiento, experiencia) orientadas a alcanzar la "obediencia en seguridad de la información", como describe Thomson y Solms 2005.

Uno de los puntos centrales de la tesis de ISCMM es que, cito en traducción propia:

> Todo intento de una organización de implementar controles técnicos y físicos de seguridad de la información sin considerar la cultura de la organización puede tener consecuencias desastrosas.

Presentan la importancia del aprendizaje gradual en este tema — Mencionan para la *incompetencia inconsciente*:

> Si los empleados ven a la seguridad de la información como un obstáculo para realizar su trabajo y no comprenden claramente el beneficio, no aceptarán la responsabilidad apropiada a su papel

> en la seguridad de la información y le "sacarán la vuelta" a toda medida de seguridad que no consideran necesaria

Sin embargo, ya que se alcanza la *competencia inconsciente* y las buenas prácticas de seguridad se convierten en *segunda naturaleza*,

> (...) la tarea se vuelve tan practicada que entra al pensamiento subconsciente del empleado y se vuelve su "segunda naturaleza" o parte de la cultura. El empleado inconscientemente competente puede incluso tener dificultades para explicar cómo se lleva a cabo determinada tarea, dado que ésta se ha convertido en instintiva.

Respecto a la relación de ISCMM con el presente trabajo, la principal observación que surge es que, a pesar de que cita ampliamente a trabajos como Mitnick y Simon 2002, parecería enfocarse a su aspecto de ingeniería social — Pero no considera que, si bien al aumentar el conocimiento y la responsabilidad relativa a la seguridad de la información mejora el nivel de defensa que pueden manejar los participantes *leales*, también aumenta la capacidad de ataque y sorpresa de los *desleales*. Considerando que, como se presentó en la Sección 5.3, 13 de los 24 los casos abordados en este trabajo están clasificados como *Acciones de personas* → *Deliberado* → *Fraude* y ocho como *Acciones de personas* → *Deliberado* → *Sabotaje*, en el dominio estudiado en particular, es indispensable no únicamente capacitar a los involucrados en esta temática, sino que crear la infraestructura de auditoría y control suficiente para dificultar que este conocimiento resulte lesivo a los fines que persigue.

5.5.5. Aplicabilidad de los modelos de madurez

Ante lo presentado en las subsecciones anteriores de la Sección 5.5, la evaluación global de la aplicabilidad de los modelos de madurez abordados a los casos estudiados no resulta halagadora: Ninguno de ellos puede ser aplicado a la información a partir de la cual se desarrolló esta investigación.

La causa primaria de dicha conclusión es la fuente de la información con que se trabajó: Partir de la descripción de un fallo en una nota periodística resulta apenas suficiente para las taxonomías desarrolladas, pero un modelo de madurez invariablemente requiere de mucha mayor información del entorno en que el fallo se produce.

El Cuadro 5.1 presenta un resumen, presentado en consonancia con el formato empleado por Igure y Williams 2008, en que se resumen las características y observaciones sobre la aplicabilidad de los cuatro modelos abordados.

Cuadro 5.1: Comparativa de los modelos de madurez presentados, relativa a los 24 incidentes estudiados.

Modelo	**Objetivos**	**Dimensión**	**Observaciones**
BSIMM (McGraw, Migues y West 2015)	Procesos de desarrollo de software	Tres niveles (numéricos, sin descripciones; propone comparativa visual con *cortes* de la industria mediante gráficas de radar	Atiende únicamente al aspecto de. desarrollo de software, no presenta una visión sistémica que permita analizar las acciones de los distintos participantes.

Continúa en la siguiente página

Continúa de la página anterior

Modelo	Objetivos	Dimensión	Observaciones
ISMM (Saleh 2011)	Manejo organizacional de seguridad informática	Cinco niveles: 1. Ningún cumplimiento; 2. Cumplimiento inicial; 3. Cumplimiento básico; 4; Cumplimiento aceptable 5; Cumplimiento pleno	Requiere mayor profundidad de información que la disponible de notas periodísticas; su aplicación requiere conocimiento de procesos internos.
CCSMM (G. B. White 2007; Sjelin y G. White 2017)	Conciencia colectiva respecto a la seguridad en una sociedad	Cinco niveles: 1. Consciente de la seguridad; 2. Desarrollo de procesos; 3. Habilitado en información; 4. Desarrollo táctico; 5. Capacidad operacional en seguridad plena	Requiere mayor profundidad de información que la disponible; su ámbito de aplicación requiere comprender la sociedad, relación entre organizaciones, no la entidad electoral por separado.
ISCMM (Thomson y Solms 2006)	Madurez corporativa a partir de la madurez agregada de cada uno de los individuos	Cinco niveles: 1. Incompetencia inconsciente; 2. Incompetencia consciente; 3. Competencia consciente; 4. Competencia inconsciente 5. Obediencia a la seguridad de la información	Modelo de madurez sólo parcialmente desarrollado; construido sobre *modelo de aprendizaje* interesante, pero no aplicado por completo; aparentemente abandonado (2006–?)

Conclusiones

Evaluando los resultados obtenidos y presentados a lo largo de este capítulo, y contrastando con los puntos planteados en el capítulo 1, se presenta la siguiente lista a modo de conclusiones:

1. *Acción humana como elemento preponderante*

   Claramente, la mayor parte de los incidentes abordados fueron causados por errores u omisiones, accidentales o determinadas, realizadas por personal con algún nivel de autorización dentro de las entidades electorales.

   Esto debe ser considerado en los modelos de ataque bajo los cuales se desarrolla la infraestructura en seguridad de las correspondientes entidades: No pueden operar bajo un modelo de defensa perimetral, siendo que las principales amenazas son internas.

   a) *Necesidad de capacitación en seguridad informática*

      Si bien, como lo demuestran las Secciones 5.3 y 5.4 la cantidad de casos en que el elemento humano primario actúa de mala fe es muy importante, la cantidad de casos debidos a la inacción por falta de guía o por omisión es alarmantemente alta.

      Resulta imperativo que el personal responsable del desarrollo, configuración y despliegue de sistemas y equipos relacionados con todas las etapas de una jornada electoral reciba capacitación especializada en seguridad informática. Debe ponerse particular atención en los puntos relacionados con los modelos de ataque relevantes al entorno problematizado.

2. *Baja disponibilidad de información*

   La mayor parte de los casos presentados se desarrollaron a partir de un mínimo de información disponible: 10 de los casos desarrollados tienen por única fuente una nota periodística. Algunos pocos son resultado de la publicación de investigación por parte de independientes, quienes documentan tan públicamente como les es posible, pero trabajando sin el aval (y muchas veces en directa oposición) de las autoridades electorales. Únicamente dos casos se realizaron como respuesta a convocatorias de auditoría limitada. No hubo *ningún* caso de auditoría pública abierta.

   a) *Importancia de las auditorías plenas, abiertas*

      En interés de la confianza que debe buscar proyectar una autoridad electoral, la seguridad de un sistema debe radicar en la fuerza de dicho sistema, y no en que éste base su operación en secretos. De ahí que se sugiere a las autoridades electorales a permitir auditorías plenas, realizadas por equipos independientes, a los algoritmos, sistemas, procedimientos, cadenas de mando y responsabilidad.

3. *Necesidad de desarrollo, validación y distribución de modelos de ataque*

   Vistos los anteriores puntos, resulta claro que las implementaciones y verificaciones oficiales se enfocan a modelos de ataque incompletos: La gran mayoría de los casos analizados, y en particular aquellos que pueden verse como más *avanzados* respecto a las conclusiones que presentamos, muestran que las fallas se presentan en escenarios no previstos en el diseño del sistema.

   Esta situación podría indudablemente mejorar si se desarrollan modelos de ataque basados en experiencias reales, como las que recoge el presente trabajo, y se consideran para el diseño de futuras implementaciones.

Trabajo futuro

Este trabajo presenta el análisis de un conjunto de fallos y, desde su planteamiento, está encaminado a facilitar el trabajo de futuras evaluaciones del voto electrónico. El trabajo realizado se limita a 24 casos, y la información disponible respecto a la mayoría es muy limitada. Es, por tanto, natural considerar como una continuación del presente trabajo:

1. A partir de los datos concentrados y presentados en este trabajo podría iniciarse el desarrollo de modelos de ataque. Su desarrollo, validación y adopción por gobiernos e industria podría redundar en un fuerte beneficio para la seguridad de futuros procesos electorales.

2. En consonancia con el segundo punto de las conclusiones, se exhorta a las autoridades electorales su evaluación ante modelos de madurez como los propuestos; si bien su aplicación resultó imposible por los puntos cubiertos en la Sección 5.5, podrían perfectamente ser cubiertos dentro de la organización.

Bibliografía

107th Congress of the United States of America (2002). *Federal Information Systems Management Act*. URL: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf (vid. págs. 11, 22).

Amato, Francisco y col. (jul. de 2015). *Vot.Ar: una mala elección*. URL: http://ivan.barreraoro.com.ar/vot-ar-una-mala-eleccion/ (visitado) (vid. pág. 61).

Amoroso, Edward G (1994). *Fundamentals of computer security technology*. Prentice-Hall, Inc. (vid. págs. 26, 28).

Aranha, Diego F. y col. (2013). *Software vulnerabilities in the Brazilian voting machine*. URL: https://sites.google.com/site/dfaranha/projects/ (visitado 25-09-2017) (vid. pág. 58).

Arora, Ashish, Rahul Telang y Hao Xu (2008). "Optimal Policy for Software Vulnerability Disclosure". En: *Management Science* 54.4, págs. 642-656. DOI: 10.1287/mnsc.1070.0771. eprint: https://doi.org/10.1287/mnsc.1070.0771. URL: https://doi.org/10.1287/mnsc.1070.0771 (vid. pág. 13).

Bingham, George Caleb (1846). *The County Election*. URL: http://homepage.cs.uiowa.edu/~jones/voting/pictures/countyelection_big.jpg (vid. pág. 14).

Bird, Larry, ed. (2004). *Vote: The Machinery of Democracy*. URL: http://americanhistory.si.edu/vote (visitado 31-07-2015) (vid. pág. 15).

Bishop, Matt (2002). *How attackers break programs, and how to write programs more securely*. SANS Institute (vid. pág. 19).

Bishop, Matt y David Bailey (1996). *A critical analysis of vulnerability taxonomies*. Inf. téc. CALIFORNIA UNIV DAVIS DEPT OF COMPUTER SCIENCE. URL: http://seclab.cs.ucdavis.edu/projects/vulnerabilities/scriv/ucd-ecs-96-11.pdf (vid. pág. 27).

Bolaños Sánchez, Ángel (nov. de 2015). *Fraude en partida participativa, acusan vecinos de Iztapalapa*. URL: http://www.jornada.unam.mx/2015/11/13/capital/045n3cap (visitado) (vid. pág. 63).

Busaniche, Beatriz (2007). "Recurso de amparo contra el voto electrónico en Río Negro". En: *Vía Libre*. URL: http://www.vialibre.org.ar/2007/12/07/recurdo-de-amparo-contra-el-voto-electronico-en-rio-negro/ (visitado) (vid. pág. 45).

— (2009). "Un investigador logra violar el secreto del voto en las urnas brasileñas". En: *Voto electrónico* 2009/12/29. URL: http://www.vialibre.org.ar/2009/12/02/un-investigador-logra-violar-el-secreto-del-voto-en-las-urnas-brasilenas/ (vid. pág. 50).

Busaniche, Beatriz y Federico Heinz (2009). *Voto electrónico: los riesgos de una ilusión*. Ed. por Vía Libre. ISBN: 978-987-22486-5-9. URL: http://www.vialibre.org.ar/wp-content/uploads/2009/03/evoto.pdf (vid. págs. 15, 33).

Caralli, Richard A y col. (mayo de 2007). *Introducing octave allegro: Improving the information security risk assessment process*. Inf. téc. CMU/SEI-2007-TR-012. DTIC Document. URL: https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419 (vid. pág. 22).

Cebula, James J, Mary E Popeck y Lisa R Young (2014). *A Taxonomy of Operational Cyber Security Risks Version 2*. Inf. téc. DTIC Document. URL: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA609863 (vid. págs. 18, 20, 69).

Chief Electoral Officer of Canada (2007). *A history of the vote in Canada*. 2.ª ed. ISBN: 0-662-44087-0. URL: http://www.elections.ca/res/his/History-Eng_Text.pdf (visitado 19-10-2016) (vid. pág. 13).

Christey, Steve (2006). *PLOVER - Preliminary List of Vulnerability Examples for Researchers*. MITRE. URL: https://cwe.mitre.org/documents/sources/PLOVER.pdf (vid. pág. 29).

Christey, Steve y Chris Wysopal (2002). "Responsible vulnerability disclosure process". En: *IETF draft* (vid. pág. 13).

Ciudad Autónoma de Buenos Aires (2014). *Reglamentación del Régimen Normativo de Elecciones Primarias, Abiertas, Simultáneas y Obligatorias*. URL: http://www2.cedom.gov.ar/es/legislacion/normas/leyes/anexos/drl4894.html (vid. págs. 17, 60).

Commission on Federal Election Reform (sep. de 2005). *Building Confidence in US Elections: Report of the Commission on Federal Election Reform*. Reporte. Center for Democracy y Election Management, American University. URL: https://www.eac.gov/assets/1/AssetManager/Exhibit%20M.PDF (vid. pág. 16).

Croarkin, Carroll, ed. (2012). *NIST/SEMATECH e-Handbook of Statistical Methods*. URL: http://www.itl.nist.gov/div898/handbook/ (vid. pág. 36).

Culp, Scott (2001). "It's Time to End Information Anarchy". En: *Microsoft Security Essay on Microsoft Technet*. URL: https://web.archive.org/web/20011109045330if_/http://www.microsoft.com:80/technet/treeview/default.asp?url=/technet/columns/security/noarch.asp (vid. pág. 13).

Curtis, Clinton Eugene (abr. de 2004). *Ohio Elections Commission*. URL: https://www.youtube.com/watch?v=u2LwnmbdiTg (visitado) (vid. pág. 41).

Dempsey, Kelly, Greg Witte y Doug Rike (2014). *Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*. National Institute of Standards y Technology. URL: http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800-53r4_summary.pdf (vid. pág. 22).

DGEQ (oct. de 2006). *Rapport d'évaluation des nouveaux mécanismes de votation*. Inf. téc. Directeur général des élections du Québec. URL: http://www.electionsquebec.qc.ca/documents/pdf/DGE-6357.pdf (visitado) (vid. pág. 43).

El Informador (mayo de 2012). "Persisten las fallas técnicas en las urnas electrónicas". En: *El Informador*. URL: http://www.informador.com.mx/primera/2012/374489/6/persisten-las-fallas-tecnicas-en-las-urnas-electronicas.htm (visitado) (vid. pág. 55).

Election Process Advisory Commission (sep. de 2007). *Voting with confidence*. Inf. téc. The Hague: Ministry of the Interior y Kingdom Relations, pág. 74. URL: http://wijvertrouwenstemcomputersniet.nl/images/0/0c/Votingwithconfidence.pdf (visitado) (vid. pág. 49).

Elizalde, Jose (1977). "Los sistemas electorales y sus repercusiones políticas: en torno a las tesis de D. Rae". En: *Revista española de la opinión pública* 48, págs. 89-113. URL: http://www.jstor.org/stable/40199478 (vid. pág. 13).

Felitti, Guilherme (nov. de 2009). "Perito quebra sigilo e descobre voto de eleitores em urna eletrônica do Brasil". En: *IDG Now!* 2010-05-28. URL: http://idgnow.uol.com.br/seguranca/2009/11/20/perito-quebra-sigilo-eleitoral-e-descobre-voto-de-eleitores-na-urna-eletronica/ (vid. pág. 50).

Felten, Ed (sep. de 2006). ""Hotel Minibar" Keys Open Diebold Voting Machines". En: *Freedom to Tinker*. URL: http://freedom-to-tinker.com/blog/felten/hotel-minibar-keys-open-diebold-voting-machines (visitado) (vid. pág. 44).

— (2008). "Evidence of New Jersey Election Discrepancies". En: *Freedom to Tinker*. URL: http://freedom-to-tinker.com/blog/felten/evidence-new-jersey-election-discrepancies (visitado) (vid. pág. 46).

Frei, Stefan y col. (2010). "Modeling the security ecosystem-the dynamics of (in) security". En: *Economics of Information Security and Privacy*. Springer, págs. 79-106. URL: http://weis09.infosecon.net/files/103/paper103.pdf (vid. pág. 13).

Geist, Michael (oct. de 2006). "Time To Cast A Vote Against E-Voting". En: *Toronto Star*. URL: http://www.michaelgeist.ca/content/view/1491/159/ (visitado) (vid. pág. 43).

Gomes, Apio (dic. de 2012). *Voto eletrônico: Hacker de 19 anos revela no Rio como fraudou eleição*. URL: https://sites.google.com/site/rcbotelhos/mercado-e-carreiras/-noticias-2010---2016/votoeletronicohackerrevelanoriocomofraudoueleicao (visitado 25-09-2017) (vid. pág. 54).

Gordon, Greg (nov. de 2008). "Glitches hamper voting in five states". En: *McClatchy DC Bureau*. URL: http://www.mcclatchydc.com/news/article24508366.html (visitado) (vid. pág. 47).

Gray, Joseph A (mar. de 1899). *Voting-machine*. US Patent 620,767 (vid. pág. 16).

Gullander, OE (1974). "Conscious Competency: The Mark of a Competent Instructor." En: *Canadian Training Methods* 7.1, págs. 20-1 (vid. pág. 77).

Halderman, Alex (2012). *Securing Digital Democracy (online course)*. URL: https://www.coursera.org/learn/digital-democracy (visitado 12-11-2015) (vid. pág. 12).

Heer, Jeffrey, Michael Bostock y Vadim Ogievetsky (2010). "A tour through the visualization zoo." En: *Communications of the ACM* 53.6, págs. 59-67. URL: https://dl.acm.org/citation.cfm?id=1743546.1743567 (vid. pág. 36).

Henríquez, Elio (dic. de 2015). *Formal prisión a manipulador de voto chiapaneco en el extranjero*. URL: http://www.jornada.unam.mx/2015/12/26/estados/024n1est (visitado) (vid. pág. 64).

Howard, John D (1997). *An analysis of security incidents on the Internet 1989-1995*. Inf. téc. Carnegie-Mellon Univ Pittsburgh PA (vid. pág. 26).

Howard, Michael, David LeBlanc y John Viega (jul. de 2005). *19 Deadly Sins of Software Security*. URL: http://www.cse.uaa.alaska.edu/~afkjm/cs470/handouts/SecuritySins.pdf (vid. pág. 19).

Hui, Zhanwei y col. (2010). "Review of software security defects taxonomy". En: *International Conference on Rough Sets and Knowledge Technology*. Springer, págs. 310-321 (vid. págs. 18, 29).

Igure, Vinay M y Ronald D Williams (2008). "Taxonomies of attacks and vulnerabilities in computer systems". En: *IEEE Communications Surveys & Tutorials* 10.1, págs. 6-19. DOI: 10.1109/COMST.2008.4483667. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4483667 (vid. págs. 18, 28, 78).

Jacobs, Bart y Wolter Pieters (2009). "Electronic Voting in the Netherlands: from early Adoption to early Abolishment". En: *Foundations of security analysis and design V*. Ed. por Springer, págs. 121-144. URL: http://www.cs.ru.nl/B.Jacobs/PAPERS/E-votingHistory.pdf (vid. pág. 16).

Janicki, Mary M. (ene. de 2003). *Mechanial lever voting machines and the Help America Vote Act of 2002*. OLR Research Report. Connecticut General Assembly. URL: https://www.cga.ct.gov/2003/olrdata/gae/rpt/2003-R-0115.htm (vid. pág. 16).

Jones, Douglas W (2010). "Early requirements for mechanical voting systems". En: *Requirements Engineering for e-Voting Systems (RE-VOTE), 2009 First International Workshop on*. IEEE, págs. 1-8. URL: http://ieeexplore.ieee.org/abstract/document/5460390/ (vid. pág. 15).

Jones, Douglas W. (2003). *A Brief Illustrated History of Voting*. URL: http://homepage.cs.uiowa.edu/~jones/voting/pictures/ (visitado 12-11-2015) (vid. pág. 13).

Joshi, Chanchala, Umesh Kumar Singh y Kapil Tarey (2015). "A Review on Taxonomies of Attacks and Vulnerability in Computer and Network System". En: *International Journal of Advanced Research in Computer Science and Software Engineering*. ISSN: 2277-128X. URL: http://www.academia.edu/download/46593781/V5I1-0273.pdf (vid. págs. 18, 29).

JTF-TI (2013). *NIST Special Publication (SP) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. URL: http://dx.doi.org/10.6028/NIST.SP.800-53r4 (vid. pág. 22).

Kerckhoff, Auguste (1883). "Desiderata de la Cryptographie Militaire". En: *Journal des sciences militaires* IX, págs. 5-38 (vid. pág. 12).

Khoury, Jack, Roni Singer-Heruti y Ofri Ilani (dic. de 2008). "Labor sets primary for tomorrow after computer failure". En: *Haaretz*. URL: http://www.haaretz.com/print-edition/news/labor-sets-primary-for-tomorrow-after-computer-failure-1.258707 (visitado) (vid. pág. 48).

Krsul, Ivan Victor (1998). *Software vulnerability analysis*. Purdue University West Lafayette, IN. URL: ftp://132.249.21.173/pub/mirrors/coast.cs.purdue.edu/pub/COAST/papers/ivan-krsul/krsul-phd-thesis.pdf (vid. págs. 26-27).

Landwehr, Carl E. y col. (1994). "A Taxonomy of Computer Program Security Flaws". En: *ACM Computing Surveys (CSUR)* 26.3, págs. 211-254. URL: http://web.cs.iastate.edu/~hridesh/teaching/610/06/02/papers/p211-landwehr.pdf (vid. pág. 26).

Lichfield, John (jun. de 2013). "Fake votes mar france's first electronic election". En: *The Independent*. URL: http://www.independent.co.uk/news/world/europe/fake-votes-mar-frances-first-electronic-election-8641345.html (visitado) (vid. pág. 56).

Lindqvist, Ulf y Erland Jonsson (1997). "How to systematically classify computer security intrusions". En: *Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on*. IEEE, págs. 154-163 (vid. pág. 26).

Lough, Daniel Lowry (2001). "A taxonomy of computer attacks with applications to wireless networks". Tesis doct. VirginiaTech. URL: https://vtechworks.lib.vt.edu/handle/10919/27242 (vid. págs. 26, 28).

Lucas, Greg (mayo de 2004). "State bans electronic balloting in 4 counties". En: *San Francisco Chronicle* A1. URL: http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/05/01/MNG036EAF91.DTL (visitado) (vid. pág. 42).

Martin, Robert A y Sean Barnum (2008). "Common weakness enumeration (cwe) status update". En: *ACM SIGAda Ada Letters* 28.1, págs. 88-91. URL: https://dl.acm.org/citation.cfm?id=1387835 (vid. pág. 29).

McGraw, Gary, Sammy Migues y Jacob West (2015). *Building Security in Maturity Model (BSIMM)*. Inf. téc. 6. Cigital. URL: https://www.inf.ed.ac.uk/teaching/courses/sp/2015/lecs/BSIMM6.pdf (vid. págs. 24, 75, 78).

Menezes, Alfred J, Paul C Van Oorschot y Scott A Vanstone (1996). *Handbook of applied cryptography*. CRC press (vid. pág. 11).

Mercuri, Rebecca T (2001). "Electronic vote tabulation checks and balances". Tesis doct. University of Pennsylvania. URL: http://repository.upenn.edu/dissertations/AAI3003665 (vid. págs. 16, 32).

Mettler, Tobias y Peter Rohner (2009). "Situational maturity models as instrumental artifacts for organizational design". En: *Proceedings of the 4th international conference on design science research in information systems and technology*. ACM, pág. 22. URL: https://dl.acm.org/citation.cfm?id=1555649 (vid. pág. 24).

Mitnick, Kevin D y William L Simon (2002). *The art of deception: Controlling the human element of security*. John Wiley & Sons (vid. pág. 78).

Nohlen, Dieter (1998). "Representación por mayoría y representación proporcional". En: *Sistemas electorales y partidos políticos*. Ed. por Fondo de Cultura Económica México D. F. Vol. 2. Cap. 5, págs. 92-134 (vid. pág. 13).

Oren, Yossef y Avishai Wool (2010). "RFID-based electronic voting: What could possibly go wrong?" En: *RFID, 2010 IEEE International Conference on*. IEEE, págs. 118-125. URL: http://www.eng.tau.ac.il/~yash/evoting-relay-rfid2010.pdf (visitado) (vid. pág. 53).

OWASP (2004). *Introduction OWASP Top Ten 2004 Project*. URL: https://www.owasp.org/index.php/Introduction_OWASP_Top_Ten_2004_Project (visitado 13-02-2017) (vid. pág. 19).

Peschard, Jacqueline (2007). *2 de julio. Reflexiones y alternativas*. UNAM. ISBN: 978-9703246359 (vid. pág. 17).

Places Chungata, Jussibeth Tatiana y col. (2017). "Confiabilidad y consideraciones del voto electrónico, una visión global". En: *Journal of Science and Research: Revista Ciencia e Investigación* 2.5, págs. 26-38. URL: http://revistas.utb.edu.ec/index.php/sr/article/view/116 (vid. pág. 33).

Polepeddi, Sriram (2005). *Software vulnerability taxonomy consolidation*. University of California, Lawrence Livermore National Laboratory. DOI: 10.2172/15020074. URL: https://e-reports-ext.llnl.gov/pdf/314682.pdf (vid. págs. 18, 28).

Prasad, Hari K. y col. (2010). "Security Analysis of India's Electronic Voting Machines". En: *17th ACM Conference on Computer and Communications Security (CCS '10)*. 2010-05-28. URL: http://indiaevm.org/paper.html (visitado) (vid. págs. 13, 51).

Ray, Bill (oct. de 2013). "Azerbaijani election app announced winner before polls even opened". En: *The Register* 2013-10-23. URL: http://www.theregister.co.uk/2013/10/09/election_app_leaks_results_ahead_of_election/ (visitado) (vid. pág. 57).

Regenscheid, Andrew y Nelson Hastings (2008). *A Threat Analysis on UOCAVA Voting Systems*. US Department of Commerce, National Institute of Standards y Technology. URL: https://www.nist.gov/sites/default/files/documents/itl/vote/uocava-threatanalysis-final.pdf (vid. págs. 18, 22, 28, 72).

Richardson, Robert (2008). *CSI computer crime and security survey*. Inf. téc. URL: http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall11/CSIsurvey2008.pdf (vid. pág. 71).

Romero Flores, Rodolfo y Julio Alejandro Téllez Valdés (2010). *Voto electrónico, derecho y otras implicaciones*. Universidad Nacional Autónoma de México. ISBN: 978-60-7021-297-0 (vid. pág. 30).

Saleh, Malik F (2011). "Information security maturity model". En: *International Journal of Computer Science and Security (IJCSS)* 5.3, pág. 21. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.207.5136&rep=rep1&type=pdf (vid. págs. 24, 79).

Saltman, R. G. (oct. de 1988). "Accuracy, Integrity and Security in Computerized Vote-tallying". En: *Commun. ACM* 31.10, págs. 1184-1191. ISSN: 0001-0782. DOI: 10.1145/63039.63041. URL: http://doi.acm.org/10.1145/63039.63041 (vid. pág. 16).

Saltman, Roy (2006). *The history and politics of voting technology: In quest of integrity and public confidence*. Springer (vid. pág. 13).

Sawer, Marian, Norman Abjorensen y Philip Larkin (2009). *Australia: The state of democracy*. Federation Press (vid. pág. 17).

Scarfone, Karen, Wayne Jansen y Tracy Miles (2008). *NIST Special Publication (SP) 800-123 Guide to General Server Security*. URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf (vid. pág. 12).

Schneier, Bruce (2007). *Full Disclosure of Security Vulnerabilities a 'Damned Good Idea'*. URL: https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html (vid. pág. 13).

Shannon, Claude (oct. de 1949). "Communication Theory of Secrecy Systems". En: *Bell System Technical Journal* 28.4 (vid. pág. 12).

Sjelin, Natalie y Gregory White (2017). "The Community Cyber Security Maturity Model". En: *Cyber-Physical Security*. Springer, págs. 161-183. URL: https://link.springer.com/chapter/10.1007/978-3-319-32824-9_8 (vid. págs. 24, 79).

Smaldone, Javier (jul. de 2015). *El sistema oculto en las máquinas de Vot.Ar*. URL: https://blog.smaldone.com.ar/2015/07/15/el-sistema-oculto-en-las-maquinas-de-vot-ar/ (visitado 30-07-2015) (vid. págs. 13, 60).

Soldevilla, Fernando Tuesta (2004). "El voto electrónico". En: *Elecciones*. Oficina Nacional de Procesos Electorales, págs. 55-80. URL: https://www.web.onpe.gob.pe/modEducacion/Publicaciones/L-0026.pdf#page=51 (vid. pág. 31).

Springall, Drew y col. (2014). "Security Analysis of the Estonian Internet Voting System". En: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. CCS '14. Scottsdale, Arizona, USA: ACM, págs. 703-715. ISBN: 978-1-4503-2957-6. DOI: 10.1145/2660267.2660315. URL: http://doi.acm.org/10.1145/2660267.2660315 (visitado) (vid. págs. 17, 59).

Stoneburner, Gary, Alice Y Goguen y Alexis Feringa (2002). *NIST Special Publication (SP) 800-30 Risk Management Guide for Information Technology Systems*. URL: https://cs.signal.army.mil/docs/sp800-30.pdf (vid. pág. 22).

Swire, Peter P (2004). "A model for when disclosure helps security: What is different about computer and network security". En: *J. on Telecomm. & High Tech. L.* 3, pág. 163. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=531782 (vid. pág. 12).

Thomson, Kerry-Lynn y Rossouw von Solms (2005). "Information security obedience: a definition". En: *Computers & Security* 2005.24, págs. 69-75. URL: https://doi.org/10.1016/j.cose.2004.10.005 (vid. pág. 77).

— (2006). "Towards an information security competence maturity model". En: *Computer Fraud & Security* 2006.5, págs. 11-15. URL: https://doi.org/10.1016/S1361-3723(06)70356-6 (vid. págs. 25, 79).

Tjøstheim, Thomas, Thea Peacock y Peter YA Ryan (2007). "A model for system-based analysis of voting systems". En: *International Workshop on Security Protocols*. Springer, págs. 114-130. URL: http://link.springer.com/chapter/10.1007/978-3-642-17773-6_13 (visitado 19-10-2016) (vid. pág. 11).

Tribunal Superior Eleitoral, Brasil (2009). *Teste de segurança do sistema eletrônico de votação*. Reporte técnico 2009/12/29. Tribunal Superior Eleitoral, Brasil. URL: https://web.archive.org/web/20101222220904/http://www.tse.gov.br/internet/urnaEletronica/seguranca.html (visitado) (vid. pág. 50).

Tripathi, Anshu y Umesh Kumar Singh (2010). "Towards standardization of vulnerability taxonomy". En: *Computer Technology and Development (ICCTD), 2010 2nd International Conference on*. IEEE, págs. 379-384. URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5645826&tag=1 (vid. págs. 18, 29).

Tsipenyuk, Katrina, Brian Chess y Gary McGraw (2005). "Seven pernicious kingdoms: A taxonomy of software security errors". En: *Security & Privacy, IEEE* 3.6, págs. 81-84. DOI: 10.1109/MSP.2005.159. URL: https://www.cigital.com/papers/download/bsi11-taxonomy.pdf (vid. págs. 18-19, 67).

— (2006). "Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors". En: *Proceedings of Workshop on Software Security Assurance Tools, Techniques, and Metrics*. Vol. 500, págs. 36-43. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.418.5789&rep=rep1&type=pdf#page=36 (vid. págs. 18, 67, 75).

Tula, María Inés (mayo de 2006). *¿Por qué la lista sábana tiene mala prensa? Un análisis sobre las consecuencias político-partidarias que trae su derogación*. Políticas Públicas Documento de Políticas Públicas Num. 25. CIPPEC. URL: http://cippec.org/oear/analisis/por-que-la-lista-sabana-tiene-mala-prensa/ (visitado 31-10-2016) (vid. pág. 15).

White, Gregory B (2007). "The community cyber security maturity model". En: *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*. IEEE, págs. 99-99. URL: http://ieeexplore.ieee.org/abstract/document/4076571/ (vid. págs. 24, 79).

WijVertrouwenStemComputersniet.nl (2009). *The Netherlands return to paper ballots and red pencils*. URL: http://wijvertrouwenstemcomputersniet.nl/English (visitado) (vid. pág. 49).

Wolchock, Scott y col. (feb. de 2012). "Attacking the Washington DC Internet Voting System". En: *16th Conference on Financial Cryptography and Data Security*. URL: https://jhalderm.com/pub/papers/dcvoting-fc12.pdf (visitado 25-09-2017) (vid. pág. 52).

Wolf, Gunnar (2011). "Voto electrónico: ¿quién tiene realmente la decisión?" En: *Seminario Construcción Colaborativa del Conocimiento*. Universidad Nacional Autónoma de México, Instituto de Investigaciones Económicas, págs. 285-301. URL: https://seminario.edusol.info/pdf/seco3_apend3.pdf (vid. pág. 34).

Xinhua (oct. de 2015). *Autoridades de Bulgaria defienden a Comisión Electoral Central de ataque cibernético*. URL: http://spanish.xinhuanet.com/2015-10/26/c_134748543.htm (visitado) (vid. pág. 62).