Ciberseguridad

El reto del siglo XXI

PARC CIENTÍFIC
VNIVERSITAT DE VALÈNCIA

Edita: Fundació Parc Científic Universitat de València
c/ Catedrático Agustín Escardino, 9
46980 Paterna (España)
Telf: +34 963544758
Correo electrónico: parc.cientific@uv.es

Coordinador: Emilio Soria-Olivas

Autores: Emilio Soria-Olivas, José Torres, Óscar Padial, Fernando Mateo, Joan Vila Francés, Manuel Domínguez, Daniel Pérez, Miguel Ángel Prada, Serafín Alonso, Antonio Morán, Juan José Fuertes, Javier Marqués, Hervé Falciani, José M. Martínez, Julio Navío, Alberto Urueña y Jorge Edo

Año: 2019

DOI: 10.7203/PCUV-2

PARC CIENTÍFIC
VNIVERSITAT DE VALÈNCIA

Indice

II. AVANCES EN MACHINE LEARNING PARA APLICACIONES DE CIBERSEGURIDAD

por Fernando Mateo, Joan Vila-Francés, Emilio Soria-Olivas

III. INTRODUCCIÓN A LA SEGURIDAD INDUSTRIAL

por Manuel Domínguez-González, Daniel Pérez-López, Miguel Ángel Prada-Madrano, Serafín Alonso-Castro, Antonio Morán-Álvarez, Juan José Fuertes-Martínez

IV. INVESTIGACIÓN Y ANÁLISIS FORENSE TECNOLÓGICO

por José Torres y Javier Marqués

V. CIBERSEGURIDAD DEL NEGOCIO Y CIBERSEGURIDAD DE LA COMPETENCIA PARA LAS PYMES

por Hervé Falciani

VI. ANÁLISIS DEL COMPORTAMIENTO DE USUARIOS DE ORDENADORES, INCIDENTES DE SEGURIDAD Y FRAUDE MEDIANTE EL USO DE SELF-ORGANIZING MAPS

por José M. Martínez-Martínez, Julio Navío-Marco, Alberto Urueña-López, Emilio Soria-Olivas

VII. ISO 27001. FUNDAMENTOS

por Jorge Edo

Prólogo

El siglo XXI es el siglo del dato, su análisis y de la conectividad; en definitiva, el siglo de la información en tiempo real y disponible para cualquiera en cualquier lugar del mundo. Dichos datos están impactando en todos los ámbitos de la sociedad y de la economía de tal forma que no se entiende ningún sector productivo ni ninguna relación social sin dato; todos tenemos algún lugar en las redes sociales desde donde intercambiamos experiencias personales o profesionales. Si a este hecho se le suma el auge de la Inteligencia Artificial, se tiene un siglo en el que los avances tecnológicos van a ser totalmente disruptivos para todos nosotros.

Sin embargo, se tienen problemas importantes que hay que resolver antes de implantar estas tecnologías. El principal es la integridad y la seguridad de la información. Sobre este último tema versa el presente volumen; la seguridad de los datos que circularán en diferentes canales, en diferentes formas y en diferentes volúmenes. No existirá un verdadero progreso mientras no se tenga un intercambio de información segura. Es tan importante este tema que Ciberseguridad se plantea como una de las profesiones del futuro. Y la otra cara de la moneda es que, a día de hoy, el uso indebido y criminal derivado de los intercambios de información mueve un volumen de dinero superior al tráfico de drogas y al tráfico de humanos juntos.

Estamos ante un gran reto del que depende el futuro de nuestra tecnología y en el que se compite entre intelectos humanos para llegar a una supremacía (plantear una seguridad completa y fiable o bien plantear sistemas/algoritmos que puedan burlar los sistemas de seguridad existentes). En este volumen se tienen diferentes aproximaciones a este mundo incipiente y con un gran futuro. Es un primer paso, pues sería necesaria una enciclopedia para ofrecer el estado del arte. Con todo, seguro que el lector lo disfrutará tanto como los que hemos sido responsables de llevarlo a cabo.

Quisiera dar las gracias en este último párrafo a los responsables del Parc Cientific de la Universitat de València por su iniciativa con estas series de libros tecnológicos; el apoyo, empuje, ayuda, entusiasmo (se me acaban las palabras) de María Iranzo para llevarlo a su finalización, ¡gracias por tu infinita paciencia!

Emilio Soria-Olivas
Catedrático del Departamento de Ingeniería Electrónica
Escola Tècnica Superior d'Enginyeria de la Universitat de València
IDAL, http://idal.uv.es

CAPÍTULO 1:

LA PERICIAL INFORMÁTICA EN EL SIGLO XXI

I. La pericial informática en el siglo XXI

POR ÓSCAR PADIAL Y JOSÉ TORRES

** Óscar Padial es Jefe de Sistemas en LESARTS, Perito e Ingeniero Técnico en Telemática y Socio Gerente de Instituto Valenciano de Ciberseguridad y Telemática.*

** José Torres es subdirector de la Escola Tècnica Superior d'Enginyeria de la Universitat de València y profesor titular del departamento de Ingeniería Electrónica.*

En los tiempos que vivimos, con un cambio tecnológico exponencial, cada vez son más comunes las continuas referencias a evidencias digitales en cualquier tipo de litigio. Sólo hace falta pensar en casos del tipo:

- Correos electrónicos aportados como evidencia de competencia desleal por parte de un trabajador, o incumplimiento del acuerdo de confidencialidad.
- Negociaciones llevadas a cabo por WhatsApp.
- Capturas de pantallas de redes sociales con vejaciones o insultos.
- Suplantación y usurpación de perfiles sociales.
- Imágenes tomadas desde un dispositivo concreto que revelan a través de sus metadatos, datos tan interesantes como la geolocalización desde donde se realizó la fotografía.

Seguro que os suenan algunos de estos casos, o incluso tenéis a algún conocido que ya ha tenido que enfrentarse al hecho de tener que aportar cualquiera de las evidencias digitales anteriormente comentadas en un proceso judicial.

Aquí es importante señalar la jurisprudencia sobre la fuerza probatoria de las capturas de pantalla tanto de correos electrónicos, como de conversaciones de WhatsApp o mensajes transmitidos a través de las redes sociales o sistemas de mensajería similares.

1. EFICACIA PROBATORIA DE CAPTURAS DE PANTALLA O PANTALLAZOS EN SEDE JUDICIAL

Como hemos comentado anteriormente, cada vez es más común que tengamos que acreditar en un juicio, a través de una captura de pantalla, lo que una persona ha escrito bien en un chat, bien en una red social, como son Twitter, Facebook o Tuenti, entre otras.

Algunos ejemplos concretos para las evidencias en formato captura de pantalla podrían ser el insulto que una persona ha verbalizado contra otra en Twitter; la apología del terrorismo o del racismo que se ha constatado dentro de una red social; o las condiciones de un contrato o despido negociado por WhatsApp.

Como sabemos, al escribir en estas redes sociales o chats, los mensajes pueden llegar a perderse con el paso del tiempo y, además en todo caso, desde el punto de vista procesal, es complicado poder exhibirlos y acreditar su contenido en un juicio. La única vía posible consiste en efectuar **capturas de pantalla** e imprimirlas (o grabarlas en un dispositivo de almacenamiento) para posteriormente aportarlas en un juicio.

Ya entrando en las afirmaciones que el Tribunal Supremo realiza sobre las conversaciones realizadas mediante los múltiples sistemas de mensajería instantánea, y que han sido objeto de titulares en varios medios, podemos destacar las siguientes:

- **Deberá tenerse cautela con este tipo de prueba:** la Sala 2ª del TS es consciente de que este tipo de archivos puede manipularse:

> *"El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo".*

En consecuencia**, se desplaza la carga de la prueba** hacia quien pretende aprovechar su idoneidad probatoria.

- **Obligación de prueba pericial:** si hay una impugnación, deberá practicarse este tipo de prueba para que se identifique el verdadero origen de esa comunicación, la fecha en la que se produjo, la identidad de los interlocutores y, en fin, la integridad de su contenido. En particular, el Tribunal Supremo expresa que:

> *El poner a disposición del Tribunal las contraseñas de acceso a la cuenta de la red social de la que se extrae la captura de pantalla o pantallazo, y practicar una pericial sobre el extremo, es una prueba contundente que acreditaría la veracidad de este tipo de conversación obrante en la captura de pantalla.*

También el Tribunal Supremo sostiene que, el aportar testigos que hayan podido comprobar la veracidad de las conversaciones que se ponen de manifiesto en la captura de pantalla, es un medio adecuado para dar credibilidad y fuerza probatoria a este tipo de prueba. Por ello, es obvio que si queremos que tenga algún valor probatorio, no basta con presentar la captura de pantalla o 'pantallazo', sino que además hay que aportar más pruebas que evidencien la veracidad de este documento y descarten su posible manipulación.

Vamos a ver un ejemplo de cómo una captura de pantalla de una red social puede manipularse con facilidad y cómo los datos que se pueden obtener al realizar la pericial pueden ser muy importantes para dar validez a dicha prueba:

Imagen 1. Supuesta captura de pantalla del perfil de Óscar Padial Díaz en Facebook. Fuente: Óscar Padial Díaz.

Imagen 2. Datos obtenidos en el análisis pericial. Se puede ver que las fechas de creación y modificación son las mismas. Fuente: Óscar Padial Díaz.

Imagen 3. Supuesta captura de pantalla del perfil de F. Juan Juan Díaz en Facebook.
Fuente: Óscar Padial Díaz

Imagen 4. Datos obtenidos en el análisis pericial donde se puede observar que las fechas de creación y modificación son distintas. Por lo tanto, se trata de un documento modificado, no original.
Fuente: Óscar Padial Díaz

No es ámbito de este capítulo entrar en más detalles sobre la realización del informe pericial en concreto, pero podemos constatar la importancia que puede llegar a tener dicho informe para que las pruebas o evidencias digitales obtenidas y presentadas en sede judicial sean tenidas en cuenta por el juez.

Por último, vamos a ver cuáles son las formas aceptadas de presentar dichas evidencias en sede judicial:

- **Fe Pública Notarial**

  Es decir, mediante un notario (fedatario público) se constatará la existencia de dichas imágenes, mensajes, correos, etc., otorgando fe pública del acceso a la cuenta de correo o del dispositivo donde esté instalada la aplicación de mensajería, y procediendo a imprimir los mensajes elegidos, los cuales se incorporarán finalmente al acta notarial.

- **Fe Pública Judicial**

  En este caso, será el Letrado de la Administración de Justicia (anteriormente el Secretario Judicial) el que levante acta del contenido concreto de las capturas de pantalla realizadas, así como del dispositivo desde donde se han realizado.

- **Realización de un Informe Pericial**

  Adicionalmente a las anteriores fórmulas de aportación de pruebas electrónicas, y como un plus de garantía de autenticidad y no manipulación, se presenta la posibilidad de practicar una prueba pericial sobre el contenido de los mensajes electrónicos y, en general, sobre cualquier otro contenido almacenado digitalmente, como pueden ser ordenadores, dispositivos móviles, páginas webs, redes sociales o similares.

En el caso concreto de las capturas de pantalla de mensajes en redes sociales también podemos utilizar lo que se denomina un notario digital. Es una figura aceptada judicialmente que, a través de un tercero, da fe del contenido de un **localizador de recursos uniforme** (más conocido por las siglas ***URL***, del inglés *Uniform Resource Locator*). Cualquier publicación en una red social es, en definitiva, una URL. Un notario digital incorporará un certificado digital y un sellado de tiempo que acredite que el contenido en ese preciso momento era el que aparecía en la captura.

Con el aumento exponencial de las nuevas tecnologías y los medios para comunicarnos a través de ellos, se amplía también exponencialmente el número de evidencias digitales a aportar y, sobre todo, aumenta su importancia sobre el veredicto final de un juez que cada día necesita apoyarse más en las evidencias digitales.

2. EFICACIA PROBATORIA DE MENSAJES DE WHATSAPP

Con el comentado aumento del uso de evidencias digitales también se extiende el riesgo de manipulación, sobre todo cuando hablamos de sistemas que en la mayoría de los casos no ofrecen ninguna garantía a la hora de identificar al usuario con una persona física.

Y en el caso concreto de mensajes de WhatsApp, las cosas se complican todavía más. Se ha publicado en numerosas investigaciones que los mensajes de WhatsApp se pueden modificar, alterando la base de datos. Entonces, ¿de qué serviría levantar un acta notarial dando fe sobre unos mensajes realizados con una aplicación que se ha demostrado que puede ser vulnerable?

De hecho, fue el propio Colegio Notarial de Valencia el que, a través de su decano, Francisco Cantos, lanzaba la negativa a realizar actas notariales que tuviesen con ellas mensajes de WhatsApp.

> *"Las conversaciones por vía de WhatsApp no son fiables ya que puede alterarse el número del remitente. Por eso, aunque podemos decir que hemos visto en una pantalla determinada conversación, no debemos asegurar que se haya producido entre una persona y otra", asegura* ***Francisco Cantos****, decano del Colegio autonómico desde el pasado mes de noviembre. "Hacen falta unos conocimientos de informática que están fuera del común de los mortales, incluidos los programadores, para saber si hay de verdad suplantación del remitente. Es imposible que el notario pueda detectarlo por sí mismo», asegura al respecto.*[1]

Vemos en el comentario anterior la importancia del informe pericial informático para acreditar el contenido de conversaciones lanzadas a través de este tipo de sistemas de mensajerías que ya forman parte de nuestro día a día y que pueden llegar a encontrar un 'limbo' en la Ley actual, pues algunas de esas aplicaciones son, incluso, más nuevas que la normativa por la que supuestamente se deben legislar.

3. LA INFORMÁTICA FORENSE

Aquí introducimos un concepto muy importante, la informática forense. Esto tiene su lógica ya que nuestra actividad como peritos se va a centrar en la mayoría de los casos en demostrar a través de la obtención de evidencias el origen de incidentes "informáticos". Para ser más exactos podemos definir la informática forense como:

> *La ciencia que se encarga del conjunto de habilidades científicas y técnicas que identifica, analiza, extrae e investiga la evidencia electrónica (informática y telemática) interpretando y determinando el origen de la causa de incidentes en medios tecnológicos (informáticos y telemáticos) de los datos potenciales y relevantes, los cuales mediante una cadena de custodia, preservamos presentados mediante un informe o dictamen; estas evidencias son muy validas y sirven para el esclarecimiento de una causa o litigio judicial o una negociación extrajudicial.*

Como peritos informáticos forenses deberemos responder a preguntas del tipo:

- ¿Quién ha realizado el ataque?
- ¿Cómo se realizó el ataque?
- ¿Qué hizo el atacante?

[1] Ortuño, Almudena (2017, 23 de enero). Los notarios valencianos rechazan levantar acta sobre las conversaciones de Whatsapp. Valencia Plaza. Recuperado de https://valenciaplaza.com/los-notarios-valencianos-se-niegan-a-levantar-acta-sobre-las-conversaciones-de-whatsapp

La informática forense es sistemática y se basa en unos hechos premeditados para recabar evidencias electrónicas para posteriormente analizarlas. El protocolo de identificación, recolección, extracción, análisis y estudio sirve para localizar y presentar de forma adecuada los hechos realizados.

No debemos confundir nuestra labor como peritos con la labor que realizan los profesionales de la seguridad informática e incluso los auditores informáticos. La informática forense no tiene parte preventiva; no se encarga de prevenir delitos sino de determinar cómo se han producido.

Como perito informático forense, se debe estar capacitado, además de en la técnica pericial específica, en la metodología a seguir y en la legislación actualizada. Esto puede parecer evidente antes de comenzar un peritaje en el sentido técnico. Por supuesto es labor del perito el aconsejar y orientar a quienes solicitan sus servicios; especialmente para poder determinar la viabilidad de la prueba. Por ejemplo, el perito informático forense valora si se ha mantenido la cadena de custodia (concepto que desarrollaremos un poco más adelante en este capítulo).

4. EL PERITO INFORMÁTICO FORENSE

El perito judicial o forense es el profesional dotado de conocimientos especializados que suministra información u opinión fundada a los tribunales de justicia sobre los puntos litigiosos que son materia de su dictamen.

El perito suministra al juez el peritaje u opinión fundada de una persona especializada en determinadas ramas del conocimiento que el juez no está obligado a dominar, a efecto de suministrarle argumentos o razones para la formación de su convencimiento. El peritaje podrá ser aportado en base a los meros conocimientos del perito, o bien a la aplicación de tales conocimientos en la evaluación de una determinada prueba. Podemos considerar, por tanto, que el perito es una persona experta en una materia a la que se recurre para que asesore en un tema relacionado con sus conocimientos.

Existen dos formas de designar a un perito para un caso:

- Peritos designados judicialmente
- Peritos designados por una de las partes

Dependiendo del tipo de designación el perito tendrá derechos y deberes que pueden variar.

4.1. PERITOS DESIGNADOS JUDICIALMENTE

- El perito tiene el derecho básico de cobrar honorarios por la elaboración del dictamen.
- El perito tiene derecho a una provisión de fondos:
  - La provisión de fondos podrá ser solicitada a cuenta de la liquidación final, en el plazo de tres días siguientes a su nombramiento.

- Si en el plazo de cinco días no se hubiere procedido al depósito, el perito quedará eximido de emitir el dictamen.

- El perito tiene el deber de aceptar el cargo que le es asignado.
- Debe respetar el código de ética que le impone su profesión y no estar inhabilitado para el ejercicio de esta.
- Debe guardar el secreto profesional cuando el caso lo imponga (acuerdo de confidencialidad).
- Debe expresar o decir la verdad con sinceridad fundamentando en todo momento las opiniones y conclusiones técnicas.

4.2. PERITOS DESIGNADOS POR UNA DE LAS PARTES

Cuando se trata de peritos de parte, el acuerdo se llega con la parte implicada y su representante legal. Aquí la figura del representante legal es clave para el perito, ya que es quién deberá apoyar su estrategia con nuestro informe pericial y sobre todo quién marcará las pautas sobre qué información debemos o no introducir en el informe. Por ejemplo, si no existe un código de conducta interno o código de confidencialidad en una empresa, es muy probable que tengamos problemas a la hora de aportar evidencias que impliquen el acceso a cuentas de usuario, aunque estos ya no formen parte de la plantilla de la empresa. Por ello, la comunicación entre el representante legal o abogado de la parte y el perito debe ser continua y clara.

Aquí el lenguaje utilizado por el perito será clave, puesto que, si el propio abogado de "nuestra parte" que tiene interés directo en entendernos no lo consigue, difícilmente lo hará el juez en caso de que toque defender el informe en sede judicial. Es importante resaltar que, a diferencia del abogado, el perito no tiene ningún interés en ninguna de las partes; su trabajo debe ser totalmente imparcial. Se trata de aportar evidencias digitales y apoyar con su trabajo las conclusiones a las que llegue. Como peritos, debe dar igual si esas conclusiones son favorables o no a la parte que nos contrata.

Las buenas prácticas del perito y la investigación se deben realizar conforme al derecho para que la investigación sea admitida y eficaz en un juicio. El perito realiza una investigación que se desarrolla a nivel de informática forense. Esta investigación debe respetar siempre la legislación vigente, los medios de prueba admitidos en derecho y la jurisdicción y competencia de los jueces y tribunales dónde deba desarrollarse la práctica tecnológica.

Por todo lo comentado hasta ahora, tiene una importancia fundamental que la figura del perito judicial suscite credibilidad y confianza. El perito judicial debe lograr tales valores mediante la adopción y la aplicación de las siguientes exigencias éticas y principios deontológicos:

- Independencia y libertad
- Lealtad e integridad
- Dignidad

- Profesionalidad, objetividad, imparcialidad y veracidad
- Capacitación y formación
- Secreto profesional y confidencialidad

5. IMPARCIALIDAD DEL PERITO

Este concepto merece mención expresa en este capítulo. La Ley de Enjuiciamiento Civil trata de asegurar la imparcialidad de los peritos a fin de que éstos no tengan ningún tipo de relación con las partes y se muestren objetivos a la hora de emitir sus conclusiones. En el caso de los peritos de parte, la imparcialidad se asegura mediante el sistema de tachas o valoración de la prueba; en caso de los peritos judiciales, se llevará a cabo por medio de la abstención o recusación.

5.1. TACHAS DE PERITOS DE PARTE

La parte contraria a aquella que ha aportado el informe pericial puede poner en entredicho la imparcialidad del perito formulando una tacha. Las circunstancias en las que puede basarse están indicadas por la ley y son las siguientes:

1. Ser cónyuge o pariente por consanguinidad o afinidad, dentro del cuarto grado civil, de una de las partes o de sus abogados o procuradores.
2. Tener interés directo o indirecto en el asunto o en otro semejante.
3. Estar o haber estado en situación de dependencia o de comunidad o contraposición de intereses con alguna de las partes o con sus abogados o procuradores.
4. Amistad íntima o enemistad con cualquiera de las partes o sus abogados o procuradores
5. Cualquier otra circunstancia, debidamente acreditada, que les haga desmerecer en el concepto profesional.

Una vez formulada la tacha, cualquier parte interesada puede dirigirse al tribunal para negar o contradecir la misma, aportando los documentos que considere pertinentes. Si la tacha perjudica a la consideración profesional o personal del perito, éste puede solicitar al tribunal que, al término del proceso, declare, mediante providencia, que la tacha carece de fundamento.

5.2. ABSTENCIÓN Y RECUSACIÓN DE LOS PERITOS JUDICIALES

Además, los peritos judiciales puedes ser recusados por otras tres causas:

1. Haber dado anteriormente sobre el mismo asunto dictamen contrario a la parte recusante, ya sea dentro o fuera del proceso.

2. Haber prestado servicios como perito al litigante contrario o ser dependiente o socio de este.

3. Tener participación en sociedad, establecimiento o empresa que sea parte del proceso.

La recusación se debe formular por medido de un escrito y se debe expresar de forma muy concreta la causa de recusación y los medios de prueba que se proponen para acreditarla. Si se estima la recusación, el perito recusado será sustituido.

Los peritos judiciales pueden ser recusados por haber dado anteriormente sobre el mismo asunto dictamen contrario a la parte recusante, ya sea dentro o fuera del proceso; por haber prestado servicios como perito al litigante contrario o ser dependiente o socio de este; y por tener participación en sociedad, establecimiento o empresa que sea parte del proceso.

6. LA VISTA ORAL

La vista oral es el lugar donde el perito debe ratificar su dictamen y aclarar las dudas que puedan surgir. Aunque no es una presencia obligatoria, es habitual ser citado para ratificar su informe y responder a las preguntas que se le realicen sobre su investigación.

Una vez que el juzgado establece una fecha para la vista oral, el perito recibirá una carta certificada citándolo para la vista oral donde se indica:

- Número de juzgado
- Información sobre las partes en conflicto
- Objeto de la citación
- Lugar, fecha y hora de la comparecencia
- Prevenciones legales. Se indican las leyes que regulan la presencia del perito, las infracciones y las sanciones aplicables.

6.1. PREPARACIÓN DE LA VISTA ORAL

Uno de los aspectos más importantes que un perito debe tener en cuenta a la hora de redactar un informe o dictamen pericial es el lenguaje utilizado. Evitar hablar con demasiados tecnicismos ayudará a la comprensión del informe.

Es muy habitual que pase tiempo entre la realización del informe y la citación judicial por lo que debemos tener el caso bien documentado y repasarlo antes. Cuando se actúa como perito de parte, el abogado y el perito se reúnen para preparar la vista y coordinar qué preguntas se realizarán y prever las cuestiones que pudiera utilizar la parte contraria. Además, es importante tener en cuenta si existen otras periciales del caso y analizar sus conclusiones.

El día de la citación el perito debe ir correctamente acreditado y con una copia de su informe donde puede tener anotaciones que puede consultar. La presencia y aspecto es un factor que no se puede descuidar, dado que la imagen que se transmite también cuenta. Se recomienda, por tanto:

- Manejo de la documentación.
- Serenidad
- Seguridad

Las principales consideraciones que el perito judicial debe tener en la vista oral serán las siguientes:

- El perito debe abstenerse de opinar.
- El perito debe ceñirse a expresar las conclusiones que se contienen en su informe evitando hablar u opinar de cualquier tema externo a su investigación.

Otros servicios que el perito puede ofrecer son la tasación y el arbitraje.

6.2. TASACIÓN

Su objetivo no es resolver una cuestión técnica, sino realizar una valoración económica aplicando conocimientos técnicos. Las tasaciones consisten en cuantificar económicamente un bien (material o inmaterial) o los daños ocasionados al mismo teniendo en cuanta su estado, antigüedad, uso, función, etc. Se realizan:

- Para empresas en quiebras, liquidaciones y cierres.
- Para juzgados en reclamaciones de daños en demandas civiles o penales, separaciones de bienes, etc.

En el entorno informático las tasaciones se centran fundamentalmente en la valoración de material o servicios.

6.3. ARBITRAJE JUDICIAL

El arbitraje, en Derecho, es una forma de resolver un litigio sin acudir a la jurisdicción ordinaria. Las partes, de mutuo acuerdo, deciden nombrar a un tercero independiente, denominado árbitro, que será el encargado de resolver el conflicto. El árbitro, a su vez, se verá limitado por lo pactado entre las partes para dictar el laudo arbitral. Deberá hacerlo conforme a la legislación que hayan elegido las partes, o incluso basándose en la simple equidad si así se ha pactado.

Vamos ahora a desarrollar un concepto clave para la actividad del perito y la realización del informe pericial.

7. LA CADENA DE CUSTODIA

La cadena de custodia es el proceso mediante el cual se garantiza la autenticidad y se conserva la integridad, tanto física como lógica, de las evidencias. Dicho de otra manera, es el nombre que recibe el conjunto de actos que tienen por objeto la recogida, el traslado y la custodia de las evidencias obtenidas en el curso de una investigación con la finalidad de garantizar la autenticidad, inalterabilidad e indemnidad de la prueba. En el caso en el que en el transcurso de las distintas acciones realizadas sobre las posibles evidencias intervengan más de una persona, debe quedar debidamente documentado.

8. PASOS A SEGUIR PARA PRESERVAR LA EVIDENCIA

Para realizar la cadena de custodia de una evidencia debemos seguir por norma general los siguientes pasos:

1. Identificación y recolección
2. Registro
3. Depósito
4. Traslado
5. Análisis final
6. Destrucción si fuese procedente

Los puntos más críticos son el 3 y 4. Por norma general cuando hablamos de periciales a empresas o particulares, durante todo el proceso es muy importante que esté presente un notario que de fe de las acciones que realiza el perito informático y que custodie las evidencias hasta el final del proceso. Para periciales judiciales existe la figura del Secretario Judicial que normalmente realiza las funciones comentadas anteriormente.

8.1. IDENTIFICACIÓN Y RECOLECCIÓN

Se deben identificar todos los equipos y sistemas a peritar y a ser posible se debe fotografiar todas las evidencias: discos duros, memorias, etc. Es habitual sacar los dispositivos del almacenamiento a peritar. Para ello también deberemos tener especial cuidado con la identificación. Se deberá documentar el número de serie, la fecha y el caso.

Han de conservarse en bolsas de seguridad que permiten almacenar el dispositivo en un ambiente antiestático y de manera precintada. De esta forma, podríamos detectar fácilmente alteraciones indebidas. Un precinto mal puesto podría romper la cadena de custodia de una evidencia.

¿Qué pasa si al realizar la investigación vemos que la prueba tiene algún fallo mecánico y no podemos obtener los datos? ¿Podemos llevarla a una empresa especializada? ¿Cómo continuamos la cadena de custodia?

Para este caso concreto, se debe realizar un documento de cadena de custodia donde se reflejará como mínimo:

- fecha y hora
- identificación de la evidencia
- origen y destino
- persona que hace entrega de la evidencia
- persona que recoge la evidencia
- estado en el que se entrega
- estado en el que se recoge

Si se trata de una pericial particular o de parte, es difícil que el cliente quiera depositar la evidencia original ante notario para que sea custodiada hasta que se realice el juicio y de esta forma se pueda garantizar la cadena de custodia. De todos modos, nosotros debemos explicar la forma correcta de realizarlo y el riesgo al que se enfrentan si no se realiza asi; si se rompe la cadena de custodia, podría llegar a invalidarse la prueba con la consiguiente pérdida de credibilidad del trabajo realizado.

9. LA EVIDENCIA DIGITAL Y TELEMÁTICA

Al principio de este capítulo hemos visto varios ejemplos de evidencias que actualmente nos podemos encontrar los peritos, pero antes de pasar a detallar algunos casos reales más, vamos a dejar claro varios aspectos muy importantes que debemos considerar antes de lanzarnos a la búsqueda o manipulación de evidencias.

Uno de esos aspectos es que debemos asegurarnos de que nuestra búsqueda no va a violar ninguna ley o dar lugar a responsabilidades legales. Las evidencias electrónicas son datos que de manera digital se encuentran almacenados o fueron transmitidos mediante equipos informáticos y que son recolectados mediante herramientas técnicas especializadas empleadas por un perito informático forense en una investigación. Tienen la función de servir como prueba física (por encontrarse dentro de un soporte) de carácter intangible (no modificable) en las investigaciones informáticas.

Un ejemplo muy claro de lo comentado en el párrafo anterior lo encontramos en los peritos informáticos especialistas en seguridad informática. Muchos de ellos en sus estudios sobre las distintas vulnerabilidades que los sistemas ofrecen o pueden ofrecer, pueden verse tentados a romper (o intentarlo) algún sistema en funcionamiento con el único afán de avisar a la empresa en cuestión de que están afectados por “X” vulnerabilidad y que deben actualizar o proteger sus sistemas. Pues bien, esto es completamente ilegal. No tenemos potestad para intentar atacar ningún sistema

a menos que estemos autorizados por la empresa en cuestión. Aunque nuestra finalidad no sea ilícita, solo podremos buscar vulnerabilidades en sistemas para los que tengamos autorización expresa.

Vamos a ver ahora varios casos prácticos en los que la figura del perito informático puede ayudar a validar las evidencias aportadas.

10. PERICIAL SOBRE UNA DIRECCIÓN IP

Uno de los casos más comunes en cualquier pericial informática forense es el de que la investigación acabe por llevarnos a una dirección IP. Lo primero que haremos es buscar el ISP (Proveedor de Servicios de internet) al que pertenece dicha dirección IP. Para esto hay multitud de herramientas en internet, incluso podemos dar con el ISP poniendo directamente la IP en el buscador de Google.

¿Y ahora? ¿Cuál es el siguiente paso? ¿Cómo puedo averiguar más datos sobre esa dirección IP? ¿Puedo saber quién hay detrás?

Este es otro de los casos típicos que comentábamos en el punto anterior. La Ley no nos autoriza a solicitar directamente información sobre una IP al proveedor de servicios de internet. En estos casos siempre tendremos que solicitar una orden judicial.

> *La Ley no nos autoriza a solicitar directamente información sobre una IP al proveedor de servicios de internet. En estos casos siempre tendremos que solicitar una orden judicial.*

Vamos a ver ahora un ejemplo práctico que se dio hace poco tiempo en el Juzgado de Instrucción número 4 de la localidad valenciana de Paterna.

Un Juzgado de Paterna (Valencia) pide información de la IP desde la que se clonó una página a favor del referéndum[2]

> *El Juzgado de Instrucción número 4 de Paterna (Valencia) ha dirigido un oficio a una compañía proveedora de servicios de internet para que identifique al titular de una IP desde la que se gestiona y administra la página web http://87.216.177.4:81/referendum.*
>
> *Este sitio web es una réplica de la página originaria www.referendum.cat, administrada y promovida por la Generalitat de Cataluña y suspendida por orden judicial.*
>
> *El Juzgado estima así la petición de la Unidad de Investigación Tecnológica de la Policía Judicial en el marco de la investigación abierta a un joven de Burjassot (Valencia) que distribuyó el código fuente a partir del cual se creó la página clonada con contenidos relacionados con*

[2] (2017, 26 de septiembre). Un Juzgado de Paterna (Valencia) pide información de la IP desde la que se clonó una página a favor del referéndum. ABC. Recuperado de https://www.abc.es/espana/comunidad-valenciana/abci-juzgado-paterna-pide-informacion-desde-clono-pagina-favor-referendum-201709261419_noticia.html

el referéndum convocado para el 1 de octubre en Cataluña y declarado ilegal por el Tribunal Constitucional.

El Juzgado de Instrucción 4 de Paterna autorizó el pasado día 23 la entrada y registro en la vivienda de este hombre, que no fue detenido. Tiene la condición de investigado en la causa abierta por desobediencia. Aún no ha sido llamado a declarar por el juez.

Según recoge el acta de entrada y registro, el joven, al que le fue facilitada copia de la parte dispositiva del auto judicial, prestó su consentimiento y colaboró voluntariamente durante la investigación en la que se intervinieron tres discos duros y un teléfono móvil.

En el momento en el que los agentes, con la preceptiva autorización judicial, realizaban el registro, el ordenador del joven estaba encendido y se estaba descargando la base de datos con los colegios electorales donde poder votar el 1-O.

En ese registro, que se circunscribió exclusivamente al dormitorio del investigado y a sus dispositivos informáticos (no se actuó sobre otros equipos que había en la vivienda, cuya propiedad atribuyó a un familiar) le fueron intervenidas temporalmente dos cuentas de correo.

El Juzgado de Instrucción 4 de Paterna no coordina ninguna otra operación relacionada con el clonado de páginas vinculadas al referéndum.

Resumiendo, en estos casos nuestra labor como peritos consistiría en llegar a la dirección IP e identificar al proveedor de servicios de internet para que a través de la correspondiente orden judicial podamos tener más información de qué persona, dirección, empresa, etc. se encuentra tras esa IP.

11. LA PERICIAL DE UN CORREO ELECTRÓNICO

Tal y como hemos estado viendo de forma continuada en este capítulo, para aportar cualquier evidencia digital esta deberá ir acompañada de su correspondiente informe pericial que ayude a validar la evidencia llegado el momento ante un juez. Un correo electrónico impreso en un papel no debería tener validez por su sencilla manipulación.

Por ello, puntos a tener en cuenta a la hora de validar un correo electrónico serían:

- Distinguir entre correo enviado o recibido
- Si el correo es enviado:
  - Acuse de recibo
  - Notario digital
- Si el correo es recibido:
  - Extracción de cabeceras

Las cabeceras de correo electrónico determinan a dónde se envía un mensaje y registran la ruta específica que sigue el correo a medida que pasa por cada servidor a través de la red. Existen múltiples aplicaciones para facilitarnos la lectura y comprensión de las cabeceras de un correo, ya que tiene muchos campos y no todos ellos son importantes.

Un resumen de los campos más importantes y su significado sería el siguiente:

From – Aquí se muestra de quién viene el mensaje. En cualquier caso, esta línea puede ser fácilmente modificada y sería la menos fidedigna.

Subject – Este contenido es lo que el remitente considera tema del correo electrónico; comúnmente se conoce como el "Asunto".

Date – En esta línea se muestra la fecha y hora en la que el mensaje fue compuesto.

To – Demuestra a quién iba dirigido el mensaje, pero podría no contener la dirección del destinatario.

Return-Path – La cuenta de correo electrónico para devolver el correo. Esto es lo mismo que "Reply-To:".

Envelope-To – Esta cabecera muestra que este correo fue enviado al buzón de correo del suscriptor del cual la cuenta de correo electrónico es destinatario@ejemplo2.com.

Delivery Date – Aquí se muestra la fecha y hora en la que el correo fue recibido por el servicio o cliente de correo.

Received – Esta cabecera es la más importante y normalmente es la de más confianza. Muestra una lista de todos los servidores/ordenadores por las que el correo ha viajado para llegar al destinatario. Las líneas "received:" se leen mejor desde abajo hacia arriba. La primera línea "received:" es tu propio sistema o servidor de correo. Y la última línea "received:" indica dónde se originó el correo. Cada sistema de correo electrónico tiene su propio estilo para mostrar las lineas "received:". Una línea "received:" general identifica la máquina que recibe el correo y la máquina desde la que se recibió el correo.

Campo SPF - Especifica qué *hosts* o direcciones IP pueden enviar correos en nombre de un dominio y las acciones a aplicar si esto no se cumple.

Campo DKIM - Firmado de los correos con una clave privada y verificación con la clave pública especificada en un registro TXT.

Campo DMARC - Especifica qué hacer con el correo en caso de fallo de las condiciones SPF ó DKIM, pudiendo eliminar el correo directamente en caso de un fallo en estos chequeos. También establece un protocolo de informes diarios para su posible posterior análisis.

12. LA PERICIAL SOBRE MENSAJES DE WHATSAPP

Aquí nos encontramos con una particularidad y es que para garantizar a ciencia cierta que un mensaje enviado ha sido recibido (en el caso que no tengamos habilitados las confirmaciones de lectura o escritura) deberíamos tener el terminal origen y el destinatario, pero ese caso no se da nunca sobre todo cuando existen demandas de por medio. El trabajo como peritos se basará en justificar que la base de datos de Whatsapp del terminal que aporta las evidencias no ha sido comprometida.

12.1. EL SECRETO DE LAS COMUNICACIONES

En muchos casos al aportar este tipo de pruebas existen serias dudas de si se está violando el derecho a la intimidad o al secreto de las comunicaciones. En este caso, es importante añadir que tal y como indica la doctrina constitucional, no hay secreto para aquel a quien se dirige la comunicación. Por lo tanto, ya sea un chat contigo únicamente, ya sea uno en el que participas dentro de un grupo, no vulnerarías el secreto a las comunicaciones.

Tal y como indica la doctrina constitucional, no hay secreto para aquel a quien se dirige la comunicación. Ya sea un chat contigo únicamente, ya sea uno en el que participas dentro de un grupo, no vulnerarías el secreto a las comunicaciones.

13. LA PERICIAL INFORMÁTICA AYUDA A IDENTIFICAR UNA RED DE BOTS O BOTNET[3]

La Sala de lo Penal de la Audiencia Nacional ha accedido a la extradición del ciudadano ruso Peter Y.L. a Estados Unidos, donde se le reclama para su enjuiciamiento por delitos de asociación delictiva para cometer fraude con ordenadores, daños informáticos, robo de identidad y escuchas electrónicas ilícitas. En este caso concreto no nos centraremos en la reclamación solicitada sobre la extradición, sino que nos sirve para ver otro ejemplo más donde podemos actuar como peritos judiciales tecnológicos.

En un auto, los magistrados de la Sección 4ª recogen los hechos por los que las autoridades americanas reclaman a Peter Y.L., detenido en Barcelona el pasado mes de abril. En esos hechos se relata cómo el reclamado controló y operó el botnet Kelihos para, entre otras cosas, recoger información personal y medios de identificación como direcciones de correo electrónico, nombres de usuarios, de acceso o contraseñas de las computadoras afectadas. Además, se usó para difundir correo basura y distribuir *software* malintencionado, incluyendo troyanos y *ransomware*.

[3] Red de ordenadores infectados con *software* malicioso

«Los ordenadores infectados como parte de cualquier y toda actividad delictuosa asociada con el bootnet Kelihos se usaron y afectaron el comercio y las comunicaciones interestatales y en el extranjero», consta en la documentación extradicional presentados por Estados Unidos. Igualmente, transmitió una comunicación que contenía una exigencia de solicitud de dinero con la intención de extorsionar a personas.

Los magistrados, una vez examinados los hechos, consideran que se dan todos los requisitos para acceder a la extradición y desestiman los argumentos presentados por la defensa de Peter Y.L. Entienden que se cumplen todos los presupuestos documentales exigidos relativos a la identidad de la persona reclamada, un resumen de las actuaciones judiciales y la orden de detención, junto con los textos legales aplicables.

Asimismo, consideran que concurren los principios de doble incriminación y mínimo punitivo, ya que si bien la defensa consideró que los hechos carecen de identidad penal pues se trata del envío de *spam* sin mayores consecuencias, la Sala señala que lejos de ello la acusación menciona haber causado pérdidas económicas, los daños cuantificados y la potencial obtención de «mucho dinero», calificado por un agente del FBI como de piratería informática y delitos relacionados con el fraude.

«Las víctimas se veían avocadas a la remisión de importe alguno para restablecer el sistema, entre otros comportamientos en la misma línea de obtención de lucro personal», explican los jueces.

En relación con la motivación política de la reclamación manifestada por el abogado de Peter Y.L, el Tribunal destaca que el procedimiento de extradición responde a la existencia de un proceso penal seguido por EEUU contra el reclamado sobre el que pesa una acusación formal emitida por el Gran Jurado del Tribunal de Distrito de Connecticut por delitos comunes «sin atisbarse la motivación política denunciada». Es otro caso más en el que la investigación de un perito judicial tecnológico puede ser de gran utilidad.

Como hemos visto durante todo este capítulo, la pericial informática en el siglo XXI es una ciencia en contínua evolución debido al cambio tecnológico exponencial que existe y que mantendrá en todo momento al perito en constante estudio de las tecnologías emergentes. Un mundo apasionante nos espera ahí fuera.

CAPÍTULO II

AVANCES EN *MACHINE LEARNING* PARA APLICACIONES DE CIBERSEGURIDAD

II. Avances en *Machine Learning* para aplicaciones de ciberseguridad

FERNANDO MATEO[a,*], JOAN VILA-FRANCÉS[a], EMILIO SORIA-OLIVAS[a]

** Fernando Mateo es profesor ayudante doctor en el departamento de Ingeniería Electrónica y miembro del grupo de investigación Intelligent Data Analysis Laboratory (IDAL) de la Universitat de València, especialista en la aplicación de métodos avanzados de aprendizaje automático.*

** Joan Vila-Francés es profesor titular del departamento de Ingeniería Electrónica y miembro del grupo de investigación Intelligent Data Analysis Laboratory (IDAL) de la Universitat de València, especialista en procesado de lenguaje natural.*

** Emilio Soria-Olivas es catedrático del departamento de Ingeniería Electrónica y miembro del grupo de investigación Intelligent Data Analysis Laboratory (IDAL) de la Universitat de València, especialista en la aplicación de métodos avanzados de aprendizaje automático.*

1. RESUMEN

En la actualidad, la seguridad informática o ciberseguridad es un área crítica en la que el aprendizaje máquina (también llamado *Machine Learning*, ML) se está volviendo cada vez más importante, especialmente dado el incremento en el número de dispositivos con conexión a internet, la frecuencia y diversidad de dichas conexiones y la negligencia de muchos usuarios que propicia vulnerabilidad en sus sistemas.

El ML tiene capacidad y versatilidad suficiente para hacer frente a estos problemas. No obstante, el uso de ML en ciberseguridad tiene asociados desafíos que conllevan un manejo metodológico y teórico de los datos. En trabajos de investigación publicados recientemente, numerosos académicos han estudiado los principales problemas de ciberseguridad existentes y han proporcionado a la comunidad de aprendizaje profundo e inteligencia artificial recomendaciones prácticas y soluciones relacionadas con el ML para ayudar a afrontar los nuevos retos en el ámbito de la ciberseguridad.

2. LOS RETOS DE LA CIBERSEGURIDAD

Con la creciente introducción en nuestra vida diaria de sistemas de visión por ordenador, reconocimiento de habla, traducción automática y muchos otros, se hace necesario hacer hincapié en la seguridad de estos sistemas para evitar que se produzcan ataques que pongan en peligro los datos personales de los usuarios.

Asimismo, la implementación a escala global de tecnologías basadas en el aprendizaje, como la publicidad digital y las infraestructuras inteligentes, la Inteligencia Artificial (IA) ha pasado de los laboratorios de investigación a la producción. Estos cambios han sido posibles gracias a la adquisición de cantidades de datos sin precedentes por el incremento en la capacidad de computación y los avances metodológicos en aprendizaje automático, por innovaciones en sistemas de *software* y arquitectura de sistemas y por la amplia accesibilidad de estas tecnologías.

La próxima generación de sistemas de IA promete acelerar estos desarrollos, que tendrán todavía más impacto en nuestras vidas a través de interacciones frecuentes con el usuario e implicarán tomas de decisiones, a menudo críticas, en nuestro nombre. Sin embargo, realizar estos avances plantea desafíos abrumadores en el diseño de los nuevos sistemas de IA [1], entre los que se pueden citar:

- Aprender continuamente al interactuar con un entorno dinámico mientras se toman decisiones que son oportunas, robustas y seguras.
- Permitir aplicaciones y servicios personalizados, sin comprometer la privacidad y seguridad de los usuarios.
- Poder entrenar los sistemas sobre conjuntos de datos propiedad de diferentes organizaciones sin comprometer su confidencialidad.

Actualmente hay una carencia de analistas de ciberseguridad cualificados y con experiencia para ayudar a minimizar el alcance y el impacto de los ataques cibernéticos globales que se producen día a día.

Además, existe una sobreabundancia de datos (big data) obtenido de numerosas fuentes que se podrían utilizar en varios algoritmos de ML para mejorar el estado actual de la ciberseguridad. Se espera que estos desarrollos de investigación ayuden a impulsar nuevos métodos que permitan afrontar la problemática existente. En concreto, un estudio de la empresa americana de ciberseguridad Webroot llevado a cabo en 2017 [2] reveló que el 74% de las empresas en los Estados Unidos y Japón ya había comenzado a utilizar algún tipo de IA o ML para proteger sus datos. Un nuevo estudio llevado a cabo en 2018 indica que un 73% de empresas planean incrementar el uso de IA/ML en sus herramientas de ciberseguridad para el año 2019 [3].

3. OPORTUNIDADES DE INVESTIGACIÓN

Frente a los retos planteados, es deseable proveer a los sistemas con fuertes propiedades de seguridad. Si bien existe una amplia gama de problemas de seguridad, se pueden distinguir dos amplias categorías. La primera categoría es un atacante que compromete la integridad del proceso de decisión. El atacante puede hacerlo, ya sea comprometiendo y tomando el control del sistema de IA en sí mismo, o alterando las entradas para que el sistema, sin saberlo, tome las decisiones que el atacante quiere. La segunda categoría es un atacante que aprende los datos confidenciales en los que se entrenó un sistema de IA, o que aprende el modelo desconocido. A continuación, discutimos tres campos de investigación prometedores [1] para defendernos contra tales ataques.

• ***Enclaves seguros.*** El rápido aumento de la nube pública y la mayor complejidad de la pila de *software* amplían considerablemente la exposición de las aplicaciones de inteligencia artificial a los ataques. Un enfoque general para hacer frente a estos ataques es proporcionar una abstracción de «enclave seguro», un entorno de ejecución seguro que protege la aplicación que se ejecuta dentro del enclave de los códigos maliciosos que se ejecutan fuera de dicho enclave.

La oportunidad de investigación en este ámbito consiste en diseñar sistemas de IA que aprovechen los enclaves seguros para garantizar la confidencialidad de los datos, la privacidad del usuario y la integridad de las decisiones, posiblemente dividiendo el código del sistema de IA entre una base de código mínima que se ejecuta dentro del enclave y el código que se ejecuta fuera del enclave. Se debe asegurar que el código dentro del enclave no filtre información, ni comprometa la integridad de la decisión.

• ***Aprendizaje adversario.*** La naturaleza adaptativa de los algoritmos de ML abre los sistemas de aprendizaje a nuevas categorías de ataques que tienen como objetivo comprometer la integridad de sus decisiones al alterar maliciosamente los datos de entrenamiento o la entrada de decisiones. Se distinguen dos categorías fundamentales: ataques de evasión y ataques de envenenamiento (*poisoning*) de datos. Los ataques de evasión tratan de generar datos que sean incorrectamente clasificados por el sistema de aprendizaje [4, 5] y por tanto, hagan que la decisión tomada sea incorrecta. Los ataques de envenenamiento de datos ocurren en la etapa de entrenamiento, donde un adversario inyecta datos “envenenados” - por ejemplo, datos con etiquetas incorrectas - en el conjunto de datos de entrenamiento que hacen que el sistema de aprendizaje aprenda el modelo incorrecto [6-8].

Para contrarrestar estos ataques se deben crean sistemas de IA que sean robustos contra las entradas adversas durante el entrenamiento y la predicción (por ejemplo, la toma de decisiones). Posiblemente podría diseñarse nuevos modelos de aprendizaje automático y arquitecturas de red aprovechando la procedencia para rastrear fuentes de datos fraudulentas y retomar decisiones después de eliminar la fuente fraudulenta.

• ***Aprendizaje compartido sobre datos confidenciales.*** Hoy en día cada compañía generalmente recopila datos individualmente, los analiza y los utiliza para implementar nuevas características y productos. Es evidente que el hecho de compartir datos puede permitir entrenar modelos más

robustos y mejor entrenados. El desafío clave del aprendizaje compartido es cómo aprender un modelo sobre datos que pertenecen a diferentes organizaciones, posiblemente competitivas, sin filtrar información relevante sobre estos datos durante el proceso de entrenamiento.

Se deben diseñar sistemas de IA que: a) puedan aprender a través de múltiples fuentes de datos sin filtrar información de una fuente de datos durante el entrenamiento, y b) puedan proporcionar incentivos a organizaciones potencialmente competidoras para que compartan sus datos o modelos.

Se deben diseñar sistemas de IA que: a) puedan aprender a través de múltiples fuentes de datos sin filtrar información de una fuente de datos durante el entrenamiento, y b) puedan proporcionar incentivos a organizaciones potencialmente competidoras para que compartan sus datos o modelos.

4. AMENAZAS FRECUENTES A UN SISTEMA INFORMÁTICO

El cibercrimen, al igual que las técnicas para afrontarlo, está en continuo desarrollo. Aunque los enfoques de ataque tradicionales (virus) cobran todavía fuerza, nuevas amenazas surgen cada día y nuevos vectores están siendo probados. En esta sección se describen algunas de las amenazas típicas a las que está expuesto un sistema informático (PC) y las posibles maneras de prevenirlas por medio de técnicas de aprendizaje automático.

4.1. *MALWARE*

El término *malware* hace referencia a programas o archivos dañinos para un sistema informático. También entrarían en esta categoría las aplicaciones potencialmente indeseadas (PUA, del acrónimo anglosajón *Potentially Unwanted Application*). El creador de uno de estos programas (atacante) intenta evitar la detección. Algunas técnicas de evasión son polimorfismo, suplantación, compresión y ofuscación [9]. Por ejemplo, el polimorfismo intenta evitar la detección de un programa generando muchas variantes y se estima que el 93% del *malware* detectado en un ordenador es polimórfico [3]. Ya que el *malware* polimórfico y las PUAs nunca tienen los mismos identificadores, las firmas existentes nunca coincidirán con la nueva variante. Esto significa que los productos de seguridad basados en coincidencia de patrones no pueden detectar nuevas variantes lo suficientemente rápido para prevenir infecciones. Una manera de detectar estas diversas variantes es basarse en la firma común del repositorio que contiene el *malware* (por ejemplo, SHA1, MD5) [10].

Una de las limitaciones para los sistemas de detección es la falta de conjuntos de datos etiquetados de manera exhaustiva. Muchas veces, los expertos etiquetan los conjuntos de datos en dominios limitados y esto conduce a la falta de muestras etiquetadas y a numerosos errores de etiquetado, conjuntos de datos desbalanceados, dificultad para identificar fuentes maliciosas y más [11].

Los sistemas de detección actuales utilizan varios algoritmos: clasificador Naive Bayes [12], Support Vector Machine [13], Random Forest [14], redes neuronales profundas [15], redes neuronales convolucionales [16], redes *long-short term memory* (LSTM) [17, 18] y otros [19-23].

En la tabla 1 se detalla la evolución del porcentaje de los archivos ejecutables considerados maliciosos, ya sean *malware* o PUA en los últimos años de acuerdo con un informe reciente de Webroot [3]. Los dispositivos analizados fueron ordenadores privados en el 68% de los casos y de empresas en el 32% restante. Se estima, además, que aparecen más de 500 millones de nuevos archivos ejecutables por año que se deben poder clasificar en tiempo real. De los datos se concluye que hay un descenso importante de las infecciones de equipos, especialmente destacable en el caso de los PUAs, debido a la mejora de los algoritmos anti-*malware*, la actualización de los sistemas operativos y a la mayor concienciación de los usuarios.

En la tabla 2 se muestra la cantidad de archivos identificados como *malware* o PUA por ordenador, y su distribución en función de si el ordenador es privado o si pertenece a una empresa o institución. El descenso en el número de archivos maliciosos es evidente, especialmente la caída producida en 2018, probablemente debida a la introducción y popularización del sistema operativo Windows 10 que incluye su propia solución antivirus Windows Defender®.

	AÑO		
	2016	2017	2018
Porcentaje de archivos ejecutables clasificados como *malware*	2.5%	1.5%	0.9%
Porcentaje de archivos ejecutables clasificados como PUA	2.2%	0.4%	0.1%

Tabla 1. Evolución temporal del porcentaje de archivos portables ejecutables (PE) analizados que son considerados indeseados. Fuente: Webroot [3].

	AÑO		
	2016	2017	2018
Número medio de archivos *malware* por ordenador	0.66	0.48	0.07
Número medio de archivos *malware* por ordenador privado	0.59	0.53	0.09
Número medio de archivos *malware* por ordenador corporativo	0.61	0.42	0.04

Tabla 2. Evolución temporal del número medio de archivos portables ejecutables (PE) analizados en un dispositivo que son considerados indeseados y su clasificación en función de si el ordenador analizado es privado o propiedad de una empresa o institución. Fuente: Webroot [3].

4.2. *RANSOMWARE*

El término *ransomware* hace referencia a un tipo de *malware* que "secuestra" cierta información, es decir, encripta la información sensible de un usuario o de una compañía y solo devuelve el control de los archivos originales después de pagar un rescate. El *ransomware* ha demostrado ser una herramienta eficaz para extraer dinero de objetivos que no estén debidamente preparados.

Este tipo de ataque tuvo especial repercusión en 2017 tras las campañas de ataques de *WannaCry* y *Petya*, que afectaron a numerosas organizaciones incluido el *National Health Service* (NHS), se extendieron a 150 países y se estima que le costaron a la economía global 6.000 millones de libras. Después de que estos ataques extendieran el miedo y el pánico a escala global, con compañías luchando para salvaguardar datos críticos y pagando millones en rescates mediante criptomoneda, la historia en 2018 fue muy diferente, con ataques aislados y a menor escala.

Uno de los vectores de ataque más habituales es el protocolo de escritorio remoto (RDP, del inglés *Remote Desktop Protocol*). Los atacantes escanean los sistemas en busca de aquellos que no tengan las medidas de seguridad necesarias y consiguen acceder a todos sus datos, así como a las unidades compartidas.

El *ransomware* se puede categorizar en dos clases principales: el *ransomware* de bloqueo niega el acceso a la computadora o dispositivo [24], y el *cryptoransomware* impide el acceso a archivos o datos. Como las muestras de *ransomware* utilizan diferentes técnicas de evasión, cualquier análisis de *ransomware* debería tener en cuenta estas técnicas [25, 26]. Los trabajos de investigación para la detección y análisis de *ransomware* pueden dividirse en enfoques estáticos y dinámicos [27]. Los enfoques estáticos confían en la firma del *ransomware* o en la utilización de una función criptográfica primitiva para la detección [28]. Los métodos dinámicos utilizan instrumentación binaria dinámica como la actividad del *ransomware* en tiempo de ejecución para la detección.

EldeRan [29] es un clasificador de *ransomware* basado en las características dinámicas de una muestra, y alcanza una tasa de verdadero positivo (TPR) de 96.3% con una baja tasa de falsos positivos (FPR) del 1.6%. UNVEIL [30] es otro sistema basado en aprendizaje automático para detección de *ransomware* que utiliza una muestra del *ransomware* interactuando con el sistema operativo, con lo que logra una TPR de 96.3% y una FPR de cero. Los comportamientos de la red y los datos de Netflow también se pueden usar para la detección de *ransomware* [31]. Otra investigación reciente [32] compara diferentes tipos de clasificadores (red bayesiana, perceptrón multicapa, árbol de decisión (J48), k-Nearest-Neighbors (kNN), Random Forest y Logistic Model Tree (LMT) para detectar *ransomware* a partir de características extraídas de conversaciones capturadas de la red, con resultados de TPR del 97.1% y FPR de 1.6% para el algoritmo J48.

4.3. *CRYPTOJACKING Y CRYPTOMINING*

El *cryptojacking* es la práctica de usar programas basados en navegador que se ejecutan a través de código incrustados en el contenido web para minar criptomoneda utilizando la CPU del usuario sin su conocimiento o consentimiento [33, 34]. El *cryptomining* se basa en la instalación de

malware que usurpa la CPU de un usuario para minar criptomoneda. Ambas técnicas han crecido rápidamente para convertirse en amenazas importantes, ya que pueden ser más lucrativas que los ataques de *ransomware* y tener una huella ilegal más pequeña.

El *cryptojacking* surgió en 2017, por lo que la mayoría de los usuarios ya han aprendido a bloquearlo. Pero la forma en que lo bloquean, utilizando complementos del navegador, es muy rudimentaria. A medida que esta amenaza evolucione y los criminales comiencen a ofuscar los dominios, esos complementos se volverán obsoletos y la detección de amenazas en tiempo real mediante IA será la única forma efectiva de bloquear a los *cryptojackers*.

Aunque no hay muchos trabajos de investigación de ML aplicado a estas técnicas dada su novedad, se han probado clasificadores basados en Random Forest con éxito en casos simulados y reales de *cryptomining,* con TPR cercanas al 100% y FPR cercanas a cero [35].

4.4. DIRECCIONES IP MALICIOSAS

Las direcciones IP maliciosas se utilizan para enviar correo no deseado, distribuir *malware*, ofuscar el origen del tráfico malicioso o permitir que los delincuentes causen estragos en las computadoras de los consumidores y las empresas. Se puede rastrear estas direcciones IP por las actividades maliciosas que realizan: escaneos, *proxies*, *spam*, *exploits* de Windows, ataques web o de denegación de servicio (DoS), *botnets*, *phishing* y amenazas a móviles. La mejor manera de abordar el peligro potencial de las IP maliciosas es bloquearlas automáticamente para que no puedan causar daños. Pero hacer esto requiere una comprensión profunda de las IP, sus ubicaciones y sus acciones para bloquearlas de manera proactiva. Además, las IPs cambian continuamente y no se puede confiar en listas estáticas de IPs a bloquear. Existen métodos basados en ML para llevar a cabo un filtrado automático de IPs [36]. Primero extraen las características de las IPs basándose en la arquitectura del protocolo IPv4 y a continuación aplican *Support Vector Machines (SVM)* para llevar a cabo la clasificación.

En estudios realizados durante 2018 se ha determinado que la amplia mayoría de las IPs maliciosas detectadas se dedican a difusión de *spam* (82%), seguidas de los *proxies* (9%) y los *botnets* (4%). Menos significativa en cuanto a porcentaje es la amenaza debida a escaneo de puertos (2%), aunque no menos peligrosa. El número de *exploits* de Windows ha disminuido drásticamente tras la introducción de Windows 10, de un 9% en 2017 a un 1.1% en 2018.

4.5. URLS MALICIOSAS

Debido al rápido crecimiento de internet, los sitios web se han convertido en el objetivo principal de los cibercriminales. Un intruso puede insertar cierto contenido malicioso en una página web con el fin de realizar actividades ilegales, tales como: sustraer información de credenciales y robo de recursos, atraer a un usuario a visitar un sitio web peligroso, descargar e instalar *software* para unirse a una *botnet* o para participar en una DoS distribuida, e incluso dañar el sistema de los visitantes. A medida que aumenta el número de páginas web, las webs maliciosas también aumentan en número y los ataques se vuelven cada vez más sofisticados.

Las empresas del sector de la seguridad informática han categorizado más de 32 mil millones de URLs hasta la fecha, examinando continuamente su historial, antigüedad, popularidad, ubicación, redes, enlaces, rendimiento en tiempo real y comportamiento. La clasificación se hace en función del propósito principal (por ejemplo, compras, sitios para adultos, juegos de azar, etc.) o intenciones maliciosas (como *phishing*, *botnets*, sitios de *malware*, sitios de *spam*, etc.), de manera que muchas de ellas se pueden filtrar por URL. Sin embargo, este enfoque heurístico basado en 'listas negras' no es óptimo, ya que los atacantes crean aliases de las URLs [37, 38] por lo que es necesario un mecanismo de detección más complejo. Una posibilidad es usar características del contenido de la página web y usarlo junto con características del léxico de la URL para posteriormente emplear un clasificador [39]. Esta posibilidad de utilizar el contenido HTML de la web junto con la URL también se aplica en herramientas de bloqueo de publicidad y páginas rastreadoras (*ad-trackers*) [40].

Existe una gran variedad de algoritmos de aprendizaje automático en la literatura que se pueden usar directamente en el contexto de la detección de URLs maliciosas. Debido a la posibilidad de que los conjuntos de datos de entrenamiento tengan un gran tamaño (millones de instancias y características), hay una necesidad de disponer de algoritmos escalables, y es por eso que los métodos de aprendizaje online han tenido mucho éxito en este dominio [41]. En concreto, se mencionan trabajos sobre aprendizaje online que emplean algoritmos de primer orden [42-45], de segundo orden [43, 46-49], Cost-Sensitive Online Learning [50, 51] y Online Active Learning [52]. También se han hecho esfuerzos para explotar el carácter disperso de los datos para mejorar el rendimiento algorítmico, así como modificar el problema a partir de un algoritmo de clasificación binaria típico para abordar el desbalanceo de clases y los problemas multiclase. Usar estas tecnologías para construir sistemas en tiempo real es otra tarea que conlleva grandes desafíos.

Debido a la gran cantidad de datos y su coste computacional asociado, las direcciones futuras de la investigación sobre detección de URLs maliciosas incluyen mejorar la extracción de características y el aprendizaje de representación (por ejemplo, mediante aprendizaje profundo) y utilizar algoritmos de entrenamiento más eficientes [41].

4.6. *PHISHING*

Refugiándose en el anonimato ofrecido por internet, los atacantes han creado nuevas técnicas, como el *phishing*, para engañar a las víctimas con el uso de sitios web falsos para recopilar su información confidencial, como identificadores de cuentas, nombres de usuario, contraseñas, etc. Se estima que el coste anual debido a ciberataques de *phishing* a empresas y usuarios puede alcanzar cifras de billones de euros [53].

El consorcio internacional *Anti-Phishing Working Group* (APWG) publica informes periódicos sobre la situación de los ataques de *phishing*. En el informe del primer trimestre de 2018 [54] destacaron que el número de dominios de *phishing* aumentan constantemente, como se puede observar en el Gráfico 1, y las páginas web fraudulentas son cada vez más elaboradas, siendo progresivamente mayor el número de ellas alojadas en dominios HTTPS e incluso las que tienen certificados SSL.

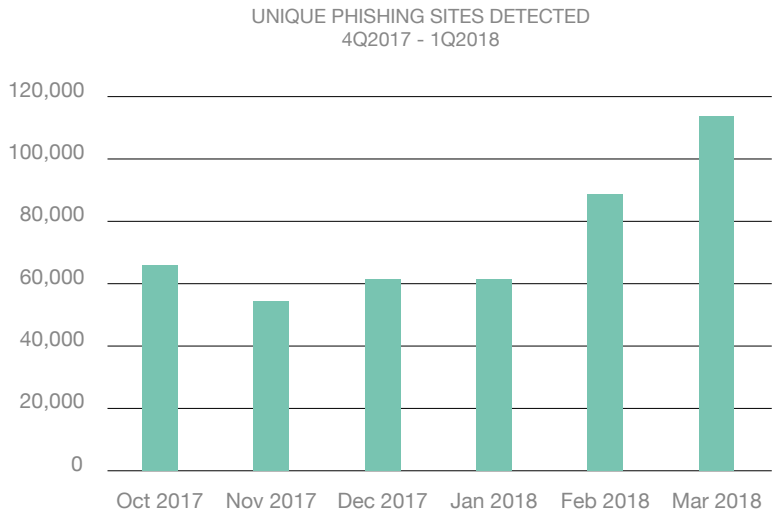


Gráfico 1. Evolución del número de sitios de phishing. Fuente: APWG

Comprender si una página web es legítima o no es un problema muy complejo debido a la estructura del ataque, basada en crear copias prácticamente idénticas a sitios web legítimos que explota la ingenuidad de los usuarios. Además, a causa del mayor uso de *smartphones*, los usuarios finales no son tan cuidadosos al verificar sus redes sociales en movimiento. Por lo tanto, los atacantes dirigen sus ofensivas principalmente a los usuarios de dispositivos móviles para aumentar la efectividad de sus ataques [55]. Es evidente que el éxito o fracaso de estos ataques depende en gran medida del nivel educativo de los usuarios en cuanto a experiencia con navegadores de internet, por tanto, muchos ataques van dirigidos a países en vías de desarrollo.

Aunque las compañías de *software* continuamente lanzan nuevos productos para combatir el *phishing* que utilizan enfoques basados en listas negras, heurísticas, aprendizaje visual y filtrado, estos productos no pueden evitar estos ataques en muchos de los casos. Es por ello necesario recurrir a sistemas de IA para diseñar sistemas *anti-phishing* con una elevada tasa de acierto en la clasificación de estos sitios y además que puedan funcionar en tiempo real.

Este es el caso de un reciente estudio [56] que plantea la detección en tiempo real de páginas web de *phishing* mediante la investigación de la URL de la página web con diferentes algoritmos de aprendizaje automático (Naive Bayes, Random Forest, kNN, Adaboost, K-star, SMO y árbol de decisión) y diferentes conjuntos de características. En primer lugar, se recopila un gran número de URLs de páginas web legítimas y fraudulentas para construir un conjunto de datos. Después, se definen tres tipos diferentes de conjuntos de características como vectores de palabras (*word vectors*), basados en procesamiento natural del lenguaje e híbridos de ambos, siendo estos últimos los que mejor resultado ofrecen utilizando el clasificador Random Forest.

4.7. AMENAZAS EN DISPOSITIVOS MÓVILES

Los teléfonos inteligentes (*smartphones*) están desplazando a los ordenadores personales como medio de acceso más frecuente a internet, ya que proporcionan una manera eficiente y conveniente de acceder, encontrar y compartir información. Sin embargo, la disponibilidad de esta información ha provocado un aumento en los ciberataques a *smartphones* en los últimos años. Actualmente, las amenazas cibernéticas van desde troyanos y virus a *botnets* y *toolkits*.

Casi la totalidad de los teléfonos inteligentes no tienen *software* de seguridad preinstalado [57]. Esta falta de seguridad es una oportunidad para que los ciberatacantes se introduzcan en los diversos dispositivos más populares (Android, iPhone y Blackberry). El *software* de seguridad tradicional que se encuentra presente en un PC, como *firewalls*, antivirus y cifrado, no tiene la misma difusión actualmente en los *smartphones*. Además, los teléfonos inteligentes son aún más vulnerables que los PC porque cada vez más personas los usan para realizar tareas vinculadas a datos sensibles. Hoy los usuarios de teléfonos inteligentes pueden enviar correos electrónicos, usar aplicaciones de redes sociales, descargar aplicaciones y realizar compras. Los usuarios ahora pueden realizar transacciones monetarias, como la compra de bienes, canje de cupones, gestión de banca online y pagos de facturas.

Desafortunadamente, la conveniencia de usar *smartphones* para realizar tareas personales significa también que los ciberatacantes tienen más oportunidades de acceder a los datos personales de manera inadvertida. Por lo tanto, es de suma importancia desarrollar políticas y estrategias a especialmente enfocadas a dispositivos móviles con el fin de proteger los datos confidenciales y personales de los usuarios.

Las transacciones monetarias son especialmente atractivas para los ciberatacantes porque pueden obtener acceso a la información de la cuenta bancaria después de hackear el smarphone de un usuario.

5. EDUCACIÓN Y CONCIENCIACIÓN DEL USUARIO

Una gran parte de la vulnerabilidad frente a ataques informáticos es debida a conductas irresponsables por parte de los propios usuarios. Más de la mitad de los usuarios que experimentan algún tipo de infección en sus equipos vuelven a sufrir otra dentro del periodo de un año [3]. Los usuarios que sufren infecciones en sus equipos de manera reiterada a menudo tienen causas basadas en el comportamiento [58].

Los usuarios que frecuentan páginas web de torrents, contenido audiovisual ilegal, trucos de juegos o claves de activación de programas están expuestos a un riesgo muy elevado de infección.

Otros de los comportamientos no recomendables es instalar aplicaciones no confiables sin examinar cuidadosamente las condiciones de su instalación.

Este riesgo podría reducirse considerablemente con una concienciación adecuada de los usuarios en conductas responsables y una educación sobre directivas básicas de comportamiento en internet como, por ejemplo, verificar que el sitio web al que lleva un enlace es legítimo antes de acceder a dicho enlace. Al educar a los usuarios a prevenir estos ataques, se facilitaría enormemente la labor de los sistemas automáticos de detección de amenazas y limpieza de equipos infectados.

6. CONCLUSIÓN

Los recientes avances en Aprendizaje Máquina y, de manera más general, de la Inteligencia Artificial, durante la última década están permitiendo desarrollar técnicas para afrontar los nuevos retos en materia de ciberseguridad de manera más eficiente. Estas técnicas automáticas son necesarias, ya que cada vez las máquinas van ganando autonomía y son capaces de tomar decisiones con poca o ninguna supervisión humana.

Gracias a los últimos avances de la Inteligencia Artificial, a la mejora constante del *software* y las nuevas funcionalidades de los sistemas operativos, se está logrando bloquear ataques informáticos tanto a servidores y ordenadores corporativos como a ordenadores personales mediante mecanismos adaptativos avanzados que no solamente utilizan 'listas negras' estáticas, sino que consiguen predecir y filtrar de manera adaptativa nuevas variantes de los métodos de ataque aprendidos. No obstante, es de gran importancia que se conciencie y eduque también al usuario de internet, puesto que navegar con una conducta responsable juega un papel muy importante en la prevención de infecciones.

7. REFERENCIAS

[1] I. Stoica, D. Song, R. A. Popa, D. Patterson, M. W. Mahoney, R. Katz, A. D. Joseph, M. Jordan, J. M. Hellerstein, J. E. Gonzalez, et al., A Berkeley view of systems challenges for ai, arXiv preprint arXiv:1712.05855.

[2] Webroot, GAME CHANGERS: AI and Machine Learning in Cybersecurity: A U.S. / Japan Comparison, https://www-cdn.webroot.com/8115/1302/ 6957/Webroot_QTT_Survey_Executive_Summary_December_2017.pdf (2017).

[3] Webroot, 2019 Webroot Threat Report, https://www-cdn.webroot.com/ 9315/5113/6179/2019_Webroot_Threat_Report_US_Online.pdf (2019).

[4] I. J. Goodfellow, J. Shlens, C. Szegedy, Explaining and harnessing adversarial examples, arXiv preprint arXiv:1412.6572.

[5] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, R. Fergus, Intriguing properties of neural networks, arXiv preprint arXiv:1312.6199.

[6] S. Mei, X. Zhu, The security of Latent Dirichlet Allocation, in: Artificial Intelligence and Statistics, 2015, pp. 681–689.

[7] S. Mei, X. Zhu, Using machine teaching to identify optimal training-set attacks on machine learners, in: Twenty-Ninth AAAI Conference on Artificial Intelligence, 2015.

[8] H. Xiao, B. Biggio, G. Brown, G. Fumera, C. Eckert, F. Roli, Is feature selection secure against training data poisoning?, in: International Conference on Machine Learning, 2015, pp. 1689–1698.

[9] I. You, K. Yim, Malware obfuscation techniques: A brief survey, 2010, pp. 297–300. doi:10.1109/BWCCA.2010.85.

[10] I. Amit, J. Matherly, W. Hewlett, Z. Xu, Y. Meshi, Y. Weinberger, Machine learning in cyber-security - problems, challenges and data sets, arXiv preprint arXiv:1812.07858.

[11] R. S. S. Kumar, A. Wicker, M. Swann, Practical machine learning for cloud intrusion detection: challenges and the way forward, in: Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, ACM, 2017, pp. 81–90.

[12] G. Luo, PredicT-ML: a tool for automating machine learning model building with big clinical data, Health information science and systems 4 (1) (2016) 5.

[13] J. Kuriakose, P. Vinod, Unknown metamorphic *malware* detection: Modelling with fewer relevant features and robust feature selection techniques, IAENG International Journal of Computer Science 42 (2) (2015) 139–151.

[14] W. Hu, Y. Tan, On the robustness of machine learning based *malware* detection algorithms, in: 2017 International Joint Conference on Neural Networks (IJCNN), IEEE, 2017, pp. 1435–1441.

[15] J. Xie, R. Girshick, A. Farhadi, Unsupervised deep embedding for clustering analysis, in: International Conference on Machine Learning, 2016, pp. 478– 487.

[16] O. E. David, N. S. Netanyahu, Deepsign: Deep learning for automatic *malware* signature generation and classification, in: 2015 International Joint Conference on Neural Networks (IJCNN), IEEE, 2015, pp. 1–8.

[17] J. Woodbridge, H. S. Anderson, A. Ahuja, D. Grant, Predicting domain generation algorithms with long short-term memory networks, arXiv preprint arXiv:1611.00791.

[18] J. Saxe, K. Berlin, eXpose: A character-level convolutional neural network with embeddings for detecting malicious URLs, file paths and registry keys, arXiv preprint arXiv:1702.08568.

[19] Z. Khorshidpour, S. Hashemi, A. Hamzeh, Learning a secure classifier against evasion attack, in: 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW), IEEE, 2016, pp. 295–302.

[20] A. M. Villegas, Function identification and recovery signature tool, in: 2016 11th International Conference on Malicious and Unwanted Software (MALWARE), IEEE, 2016, pp. 1–8.

[21] N. McLaughlin, J. Martinez del Rincon, B. Kang, S. Yerima, P. Miller, S. Sezer, Y. Safaei, E. Trickel, Z. Zhao, A. Doupé, et al., Deep android *malware* detection, in: Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, ACM, 2017, pp. 301–308.

[22] W. Hu, Y. Tan, Generating adversarial *malware* examples for black-box attacks based on GAN, arXiv preprint arXiv:1702.05983.

[23] O. Patri, M. Wojnowicz, M. Wolff, Discovering *malware* with time series shapelets, in: Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.

[24] K. Savage, P. Coogan, H. Lau, The evolution of ransomware, Tech. rep., Symantec (2015).

[25] F. Mercaldo, V. Nardone, A. Santone, Ransomware inside out, in: 2016 11th International Conference on Availability, Reliability and Security (ARES), IEEE, 2016, pp. 628–637.

[26] K. Liao, Z. Zhao, A. Doupé, G.-J. Ahn, Behind closed doors: measurement and analysis of cryptolocker ransoms in bitcoin, in: 2016 APWG Symposium on Electronic Crime Research (eCrime), IEEE, 2016, pp. 1–13.

[27] D. D. Hosfelt, Automated detection and classification of cryptographic algorithms in binary programs through machine learning, arXiv preprint arXiv:1503.01186.

[28] S. Ranshous, S. Shen, D. Koutra, S. Harenberg, C. Faloutsos, N. F. Samatova, Anomaly detection in dynamic networks: a survey, Wiley Interdisciplinary Reviews: Computational Statistics 7 (3) (2015) 223–247.

[29] D. Sgandurra, L. Muñoz-González, R. Mohsen, E. C. Lupu, Automated dynamic analysis of ransomware: Benefits, limitations and use for detection, arXiv preprint arXiv:1609.03020.

[30] A. Kharaz, S. Arshad, C. Mulliner, W. Robertson, E. Kirda, UNVEIL: A large-scale, automated approach to detecting ransomware, in: 25th USENIX Security Symposium (USENIX Security 16), 2016, pp. 757– 772.

[31] K. Cabaj, P. Gawkowski, K. Grochowski, D. Osojca, Network activity analysis of cryptowall ransomware, Przeglad Elektrotechniczny 91 (11) (2015) 201–204.

[32] O. M. Alhawi, J. Baldwin, A. Dehghantanha, Leveraging machine learning techniques for Windows ransomware network traffic detection, Cyber Threat Intelligence (2018) 93–106.

[33] S. Eskandari, A. Leoutsarakos, T. Mursch, J. Clark, A first look at browser-based cryptojacking, in: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE, 2018, pp. 58–66.

[34] M. Saad, A. Khormali, A. Mohaisen, End-to-end analysis of in-browser cryptojacking, arXiv preprint arXiv:1809.02152.

[35] D. Carlin, P. O'kane, S. Sezer, J. Burgess, Detecting cryptomining using dynamic analysis, in: 2018 16th Annual Conference on Privacy, Security and Trust (PST), IEEE, 2018, pp. 1–6.

[36] D. Chiba, K. Tobe, T. Mori, S. Goto, Detecting malicious websites by learning IP address features, in: 2012 IEEE/IPSJ 12th International Symposium on Applications and the internet, 2012, pp. 29–39. doi:10.1109/SAINT. 2012.14.

[37] S. Chhabra, A. Aggarwal, F. Benevenuto, P. Kumaraguru, Phi.sh$oCiaL: the phishing landscape through short urls, in: Proceedings of the 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference, ACM, 2011, pp. 92–101.

[38] Y. Alshboul, R. Nepali, Y. Wang, Detecting malicious short URLs on Twitter, in Twenty-first Americas Conference on Information Systems, Puerto Rico, 2015

[39] A. Sirageldin, B. B. Baharudin, L. T. Jung, Malicious web page detection: A machine learning approach, in: H. Y. Jeong, M. S. Obaidat, N. Y. Yen, J. J. J. H. Park (Eds.), Advances in Computer Science and its Applications, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 217–224.

[40] U. Iqbal, Z. Shafiq, P. Snyder, S. Zhu, Z. Qian, B. Livshits, Adgraph: A machine learning approach to automatic and effective adblocking, arXiv preprint arXiv:1805.09155.

[41] D. Sahoo, C. Liu, S. C. Hoi, Malicious URL detection using machine learning: a survey, arXiv preprint arXiv:1701.07179.

[42] J. Ma, L. K. Saul, S. Savage, G. M. Voelker, Learning to detect malicious URLs, ACM Transactions on Intelligent Systems and Technology (TIST) 2 (3) (2011) 30.

[43] J. Ma, L. K. Saul, S. Savage, G. M. Voelker, Identifying suspicious URLs: an application of large-scale online learning, in: Proceedings of the 26th annual international conference on machine learning, ACM, 2009, pp. 681– 688.

[44] W. Zhang, Y.-X. Ding, Y. Tang, B. Zhao, Malicious web page detection based on on-line learning algorithm, in: 2011 International Conference on Machine Learning and Cybernetics, Vol. 4, IEEE, 2011, pp. 1914–1919.

[45] K. Thomas, C. Grier, J. Ma, V. Paxson, D. Song, Design and evaluation of a real-time URL spam filtering service, in: 2011 IEEE Symposium on Security and Privacy, IEEE, 2011, pp. 447–462.

[46] A. Blum, B. Wardman, T. Solorio, G. Warner, Lexical feature based phishing URL detection using online learning, in: Proceedings of the 3rd ACM Workshop on Artificial Intelligence and Security, ACM, 2010, pp. 54–60.

[47] A. Le, A. Markopoulou, M. Faloutsos, Phishdef: URL names say it all, in: 2011 Proceedings IEEE INFOCOM, IEEE, 2011, pp. 191–195.

[48] J. Ma, A. Kulesza, M. Dredze, K. Crammer, L. Saul, F. Pereira, Exploiting feature covariance in high-dimensional online learning, in: 13th International Conference on Artificial Intelligence and Statistics (AISTATS), 2010.

[49] M.-S. Lin, C.-Y. Chiu, Y.-J. Lee, H.-K. Pao, Malicious URL filtering—a big data application, in: 2013 IEEE international conference on big data, IEEE, 2013, pp. 589–596.

[50] J. Wang, P. Zhao, S. C. Hoi, Cost-sensitive online classification, IEEE Transactions on Knowledge and Data Engineering 26 (10) (2013) 2425–2438.

[51] P. Zhao, S. C. Hoi, Cost-sensitive online active learning with application to malicious URL detection, in: Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM, 2013, pp. 919–927.

[52] S. C. Tice, Classification of Web Pages in Yioop with Active Learning. Master's thesis, San Jose State University (2013).

[53] A. N. Shaikh, A. M. Shabut, M. Hossain, A literature review on phishing crime, prevention review and investigation of gaps, in: 2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), IEEE, 2016, pp. 9–15.

[54] APWG, Phishing Activity Trends Report: 1st Quarter 2018, https:// docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf (2018).

[55] D. Goel, A. K. Jain, Mobile phishing attacks and defence mechanisms: State of art and open research challenges, Computers & Security 73 (2018) 519–544.

[56] O. K. Sahingoz, E. Buber, O. Demir, B. Diri, Machine learning based phishing detection from URLs, Expert Systems with Applications 117 (2019) 345–357.

[57] J. Wright, M. E. Dawson Jr, M. Omar, Cyber security and mobile threats: The need for antivirus applications for smart phones, Journal of Information Systems Technology and Planning 5 (14) (2012) 40–60.

[58] A. Urueña-López, F. Mateo, J. Navío-Marco, J. M. Martínez-Martínez, J. Gómez-Sanchís, J. Vila-Francés, A. J. Serrano-López, Analysis of computer user behavior, security incidents and fraud using self-organizing maps, Computers & Security 83 (2019) 38–51.

CAPÍTULO III

INTRODUCCIÓN A LA SEGURIDAD INDUSTRIAL

III. Introducción a la ciberseguridad industrial[1]

POR MANUEL DOMÍNGUEZ GONZÁLEZ, DANIEL PÉREZ LÓPEZ, MIGUEL ÁNGEL PRADA MEDRANO, SERAFÍN ALONSO CASTRO, ANTONIO MORÁN ÁLVAREZ, JUAN JOSÉ FUERTES MARTÍNEZ

** Los autores son miembros del Departamento de Ingeniería Eléctrica y de Sistemas y Automática de la Universidad de León.*

1. INTRODUCCIÓN

Las tecnologías de información y comunicaciones han supuesto uno de los mayores avances tecnológicos con un gran impacto en la sociedad. Este impacto ha aumentado por la gran cantidad de dispositivos conectados a la red, no sólo por la explosión de *smartphones* y *tablets*, sino también por la conexión de otros dispositivos en el denominado internet de las Cosas (*internet of Things*, IoT) (Sisinni et al., 2018), lo cual nos lleva a un paradigma de conectividad que incluso ha transformado nuestro comportamiento cotidiano. Nos encontramos así con una integración entre dispositivos mediante mecanismos como los sistemas ciber-físicos (E. A. Lee 2008), cuya computación está estrechamente interrelacionada con el proceso físico global y sus partes distribuidas están comunicadas y coordinadas entre sí.

Por otra parte, avances como la Inteligencia Artificial, el aprendizaje automático o el *big data* conllevan grandes cambios tecnológicos que han transformado la interacción de los humanos con la información. La enorme cantidad de sensores disponibles, en combinación con la gran potencia analítica actual, da lugar a avanzados dispositivos 'inteligentes' que aportan información y nuevas funcionalidades de forma rápida y eficiente. Esto, aplicado a un entorno industrial, abre la posibilidad de una 'fábrica inteligente', con mayor flexibilidad frente a las necesidades y procesos de producción y una asignación eficiente de recursos, lo que da lugar a una cuarta revolución industrial o *Industria 4.0*, término acuñado por la Academia Alemana de Ciencia e Ingeniería, cuya equivalencia en España se conoce como iniciativa Industria Conectada 4.0.

La Industria 4.0 se sustenta fundamentalmente en la digitalización industrial y la coordinación cooperativa entre todos sus elementos interconectados (Lu, 2017; J. Lee, Bagheri, and Kao, 2015). Con la inclusión de numerosas tecnologías como, por ejemplo, el internet industrial de las cosas (*Industrial internet of Things*, IIoT) (Da Xu, He and Li, 2014; Sisinni et al., 2018) o la computación en la nube, sus principales metas son alcanzar mayor eficiencia operacional y productividad. Por tanto, existen numerosos beneficios potenciales para las empresas, que van desde mejoras de la calidad en sus productos con bajos costes hasta una optimización en su propia organización, pasando por menores tiempos de inactividad. Sin embargo, el potencial que aporta la integración ofrecida por la Industria 4.0 conlleva también riesgos, ya que nuevas ciberamenazas emergen

[1] Este trabajo fue financiado por el gobierno de Castilla y León y por el Fondo Europeo de Desarrollo Regional bajo el proyecto LE045P17.

continuamente. Por ejemplo, el espionaje industrial ya no sólo ocurre mediante un acceso físico no autorizado a los datos de una planta industrial, sino también cuando el nexo entre tecnologías de información (IT) y de operación (OT) se ve comprometido.

Los sistemas autónomos conectados a redes industriales susceptibles a sabotaje suponen un peligro, sobre todo si afectan a servicios básicos, tales como la electricidad o la salud, gestionados en infraestructuras críticas. Ya existen ejemplos emblemáticos de materialización de dichas amenazas con graves consecuencias, como el incidente Stuxnet[2] o el de la red eléctrica ucraniana[3]. El aumento de este tipo de ataques a sistemas de control demuestra la vulnerabilidad de la industria y la consecuente necesidad de mejorar su ciberseguridad (Cardenas et al., 2009).

En este punto es importante diferenciar entre la seguridad operacional (*safety*) y la seguridad (*security*); la primera engloba la reducción de incidentes derivados de la operación, como eventos accidentales con daños materiales y/o personales, desastres naturales, errores humanos, etc. y la segunda apunta a la protección ante daños intencionados como actos de sabotaje y robo, entre otros. Esta última incluye la seguridad física y la ciberseguridad. La seguridad operacional y la seguridad física siempre han sido tenidas en cuenta en los sistemas de control, al contrario que la ciberseguridad. El énfasis en la relevancia de la ciberseguridad industrial y la mayor parte de los avances son relativamente recientes en relación a otros sistemas de información.

Aunque existe una larga trayectoria en ciberseguridad para el campo IT, no se podrían aplicar directamente todos sus métodos en el área OT por varias razones como, por ejemplo, la diversidad de las tecnologías utilizadas, los requisitos de tiempo real y la presencia habitual de dispositivos obsoletos, entre otros motivos (V. Stouffer, Lightman, and Hahn, 2015). Esto hace que, en este caso, la prioridad de los objetivos de seguridad cambie, siendo clave en primer lugar la disponibilidad del proceso, después la integridad y finalmente la confidencialidad.

Por todo lo anterior, en este capítulo se realiza una revisión en el campo de la ciberseguridad industrial, analizando las vulnerabilidades y amenazas que pueden poner en riesgo sistemas de control, su impacto en el área de las infraestructuras críticas y la normativa existente. Asimismo, se indican varias recomendaciones a considerar, así como propuestas de experimentación y formación en esta materia.

2. SISTEMAS DE CONTROL INDUSTRIALES

Un sistema de control industrial es una combinación de varias configuraciones y componentes para alcanzar un objetivo industrial de automatización y control de un proceso. Las principales tareas de su funcionamiento consisten en funciones de supervisión del estado del proceso y el propio control, cuyas acciones realizan cambios en el proceso.

[2] Más información en la página 54.
[3] Más información en la pagina 55.

Situaciones habituales, como la interconexión con redes corporativas, accesos remotos y conexión de medios externos, provocan que actualmente la superficie de ataque sea amplia.

Se utilizan diversos elementos como los controladores lógicos programables (*Programmable Logic Controllers*, PLC), que son dispositivos de control optimizados para trabajar con múltiples entradas y salidas donde se recogen datos de los sensores y se envían acciones de control para los actuadores (Mandado Pérez, Marcos Acevedo, and Fernández Silva, 2009). También se hace uso de sistemas de control distribuidos (*Distributed Control Systems*, DCS), frecuentemente utilizados en automatizaciones complejas como en industrias petroquímicas, incluyendo robustez y redundancia. Por su parte, los sistemas instrumentados de seguridad (*Safety Instrumented Systems*, SIS) o de parada de emergencia están enfocados a la seguridad operacional, que pueden llevar a un estado seguro predefinido. En cuanto a la supervisión, se utilizan interfaces hombre-máquina (*Human Machine Interfaces*, HMI) y los sistemas de supervisión, control y adquisición de datos (*Supervisory Control And Data Acquisition*, SCADA), que permiten visualizar el proceso, permitiendo la inspección y manipulación de sus variables, así como la recepción de alarmas.

Además de las habituales arquitecturas piramidales de automatización, como el modelo *Purdue Enterprise Reference Architecture*, en el cual la arquitectura empresarial se divide en varios niveles, existe la tendencia actual en la industria de aumentar la conectividad y la integración con los servicios IT, como servicios web (máquina a máquina, M2M), el análisis de datos o la Inteligencia Artificial para la mejora del proceso y producto. El *Reference Architecture Model Industry* 4.0 (RAMI 4.0) propone un modelo unificado que incluye los componentes de la Industria 4.0 de manera estructurada, en la cual no existe tanta diferenciación entre los niveles anteriormente incluidos en la pirámide.

La integración de los sistemas de control con otros sistemas de información es ya habitual desde hace años. El hecho de que estos sistemas hayan dejado de trabajar de manera aislada ha expuesto varias deficiencias en términos de seguridad. De hecho, el aumento de las vulnerabilidades e incidentes de ataques ha motivado que la ciberseguridad industrial se haya convertido en un asunto de interés. Por ejemplo, los fabricantes incluyen elementos de seguridad y ha aumentado el desarrollo de normativa relacionada. Sin embargo, su nivel de madurez es menor que en otros ámbitos y el desarrollo de procedimientos incluye a numerosos agentes como fabricantes, usuarios o administraciones. Para mejorar dichos aspectos, existen todavía retos en concienciación, formación y desarrollo de procedimientos y tecnologías adecuadamente adaptados a los requisitos de estos sistemas.

Desde el punto de vista de la seguridad, si el atacante puede manipular la entrada del proceso, la monitorización de alguna variable relacionada con alarmas o directamente el control, pueden darse situaciones no deseadas con graves consecuencias. Además, existen ciertas particularidades en los sistemas de control que las hacen diferentes a otros sistemas de información.

La longevidad de las instalaciones y, consecuentemente, las tecnologías obsoletas dependientes de los fabricantes, ofrecen una protección posiblemente limitada con difícil gestión de mantenimiento y parcheo.

Por otra parte, a diferencia de otros sistemas, la disponibilidad es más importante que la integridad y la confidencialidad, puesto que una pérdida de disponibilidad no solo implicaría consecuencias económicas, sino también posibles fallos en el proceso. Por ejemplo, un retardo en las comunicaciones podría afectar a la supervisión del proceso, a una saturación del dispositivo o incluso a un bloqueo que lo inutilice, pudiendo provocar daños materiales. Esta alta prioridad de la disponibilidad impone limitaciones a la introducción de modificaciones y prácticas que perturben el funcionamiento del proceso.

Entre las comunicaciones requeridas en la automatización de procesos, podemos en primer lugar destacar los protocolos de bus de campo, como Modbus RTU, PROFIBUS o DeviceNet (CIP), que se utilizan para conectar los equipos de control con la instrumentación de campo como, por ejemplo, un PLC a un determinado sensor. Generalmente son protocolos en serie y, debido a su antigüedad, no fueron diseñados desde una perspectiva de seguridad, por lo que carecen de cualquier medida inherente de seguridad como autenticación, cifrado, etc. Los protocolos a nivel de control, que permiten comunicar los dispositivos de control entre sí o con elementos de supervisión, son a menudo simples extensiones de los protocolos de bus de campo para operar en redes Ethernet sobre la pila TCP/IP. De esta manera, podemos encontrarnos protocolos como Modbus TCP, PROFINET o Ethernet/IP (CIP) que, al igual que sus homólogos, de bus de campo, carecen de medidas de seguridad.

Adicionalmente, también es común el uso de protocolos propietarios o extensiones no documentadas basadas en protocolos abiertos para la configuración de los autómatas desde las estaciones de ingeniería. En este caso, a la ausencia de seguridad anteriormente citada se une además el desconocimiento. Por tanto, es absolutamente necesario realizar una estricta segmentación de redes e incluir elementos de detección y filtrado que descubran y bloqueen comunicaciones no deseadas en la zona industrial.

Es absolutamente necesario realizar una estricta segmentación de redes e incluir elementos de detección y filtrado que descubran y bloqueen comunicaciones no deseadas en la zona industrial.

Para la interconexión de elementos de control y supervisión de diversos fabricantes también es muy común el estándar *OLE for Process Control* (OPC) que, en su versión clásica, utilizaba tecnologías OLE, COM y DCOM desarrolladas por Microsoft. Esta implementación posee varias deficiencias de seguridad, que permiten el acceso directo a registros de dispositivos de la mayoría de vendedores

sin autenticación, confidencialidad e integridad. Por ello, la fundación OPC ha propuesto una nueva versión más segura, la *OPC Unified Architecture* (OPC UA), independiente de la plataforma, con codificación y autenticación segura y extensible a nuevas funcionalidades.

En otras aplicaciones no industriales de los sistemas de control encontraremos diferentes tecnologías de comunicación. Por ejemplo, en los sistemas de gestión de edificios, que controlan funcionalidades como la iluminación o los sistemas de calentamiento, ventilación y aire acondicionado, se pueden encontrar protocolos como KNX, BACnet o, de nuevo, Modbus. Suelen, no obstante, tener las mismas deficiencias de seguridad, incluyendo, por ejemplo, mensajes sin cifrar. Ello es problemático puesto que normalmente el personal involucrado en su operación es menos numeroso y peor formado. Donde sí se detecta una evolución mayor es en los protocolos utilizados para el control del transporte y distribución de la energía eléctrica, donde el moderno estándar IEC 61850, que está siendo progresivamente implantado en toda Europa, ha sido concebido considerando la seguridad en su diseño.

3. INFRAESTRUCTURAS CRÍTICAS

Los sistemas de control son un elemento clave en las instalaciones que proporcionan servicios esenciales básicos en sectores estratégicos. Los sistemas y recursos, físicos o lógicos, en los que cualquier interrupción supone un gran impacto en la sociedad, se consideran infraestructuras críticas y su protección es de gran importancia para el funcionamiento normal de los estados y el bienestar de sus ciudadanos (Alcaraz and Zeadally, 2015). En la actual normativa española hay 12 áreas diferenciadas, entre las que se incluyen las infraestructuras energéticas y de distribución de agua, el transporte o el eficaz funcionamiento de las instituciones esenciales del Estado.

Gráfico 1. Los sectores estratégicos en España divididos por áreas. Fuente: propia.

La conexión existente entre estos sectores hace que una infraestructura crítica pueda depender de los servicios de otra u otras, lo cual puede producir efectos en cascada en caso de algún fallo en alguna de ellas. Estas interdependencias fueron catalogadas (Rinaldi, Peerenboom and Kelly 2001) en físicas, cuando se requieren recursos materiales de otra infraestructura; geográficas, cuando comparten una localización próxima y un problema en una de ellas pueda afectar a la otra; ciber-dependencias, como resultado de sistemas de comunicación e información; y lógicas, cuando se encuentran conectadas por un agente diferente a los anteriores.

4. AMENAZAS, VULNERABILIDADES Y RIESGOS EN EL ÁMBITO INDUSTRIAL

Los dispositivos industriales están diseñados para un determinado rendimiento, fiabilidad y durabilidad diferente a los de una red empresarial, lo que puede dificultar la gestión de su seguridad. Además de las medidas de seguridad operacional siempre presentes, muchos sistemas industriales cuentan con medidas de seguridad física, pero la seguridad de su información no siempre fue una prioridad. Inicialmente no era crítica, puesto que estos sistemas se encontraban físicamente aislados para su funcionamiento. La progresiva integración entre las tecnologías de información y operación (IT/OT) ha llevado a que esa separación vaya desapareciendo. Situaciones habituales, como la interconexión con redes corporativas, accesos remotos y la conexión de medios externos, provocan que actualmente la superficie de ataque sea amplia, lo que obliga a estudiar exhaustivamente las amenazas y vulnerabilidades antes de tomar medidas.

Las amenazas son las posibles acciones que pueden producir un daño en el sistema, provocando una pérdida de confidencialidad, integridad y/o disponibilidad del mismo, de sus datos o aplicaciones que, como resultado, conlleve consecuencias indeseables, a nivel físico, de funcionalidad, reputacional o económico. Estas amenazas son muy variadas: de fuentes internas o externas, intencionadas o no, dirigidas o de carácter general.

Los principales activos susceptibles a amenazas son equipos, productos, información del proceso, red o incluso personal. Las fuentes de una amenaza se deben conocer correctamente para definir e implementar medidas adecuadas. Las más probables son las internas, realizadas por agentes como empleados malintencionados o insuficientemente formados, y las de terceros (clientes o proveedores) con acceso a ciertos activos. Con todo, en función de la relevancia del proceso o la infraestructura bajo control, tampoco pueden descartarse amenazas externas de agentes con intereses económicos o estratégicos (ciberterrorismo, espionaje, etc.).

Los ataques remotos de carácter dirigido requieren a menudo de un alto grado de especialización y, como vectores de entrada a los sistemas de control, incluyen métodos como *phishing* (e-mails personalizados para engañar al destinatario mediante enlaces o adjuntos con el objetivo de que inicie *malware* inadvertidamente), *watering hole* (código malicioso inyectado en webs que el personal de planta suele visitar con el mismo objetivo) o la inyección maliciosa de consultas en bases de datos accesibles en la red perimetral.

Una vez infiltrado en la red, de forma manual o por medio de *malware*, el atacante intentará pivotar entre dispositivos y redes hasta propagarse a las redes donde se encuentra el objetivo de interés. En el caso de las redes industriales, esto puede suponer el acceso no autorizado o la interrupción del servicio de elementos de la red de supervisión o de planta. Es habitual en estos casos hablar de amenaza persistente avanzada o APT (*Advanced Persistent Threat*), un concepto que engloba un conjunto de procesos, continuados en el tiempo y orientados a atacar una entidad determinada -normalmente organizaciones o naciones-, haciendo uso de sofisticadas técnicas para adquirir información relevante del objetivo, permanecer oculto pero operativo e interrumpir el funcionamiento de objetivos muy concretos.

Respecto a los sistemas de control, las amenazas específicas a sus elementos incluyen: la denegación de servicio; interceptar las comunicaciones, configuraciones y/o datos; alterar las aplicaciones y sus registros de actividad (*logs*); eludir la autenticación y políticas de permisos y robar credenciales. Los elementos de control pueden ser sometidos a una alteración de su *firmware* o del modo de ejecución -por ejemplo, una parada-, o a la interceptación/alteración de la estrategia de control para observar o modificar su actividad. Por otra parte, las amenazas más críticas en los elementos de supervisión afectan a la integridad y autenticidad de los datos de explotación o de sus comunicaciones hacia los niveles de control o gestión.

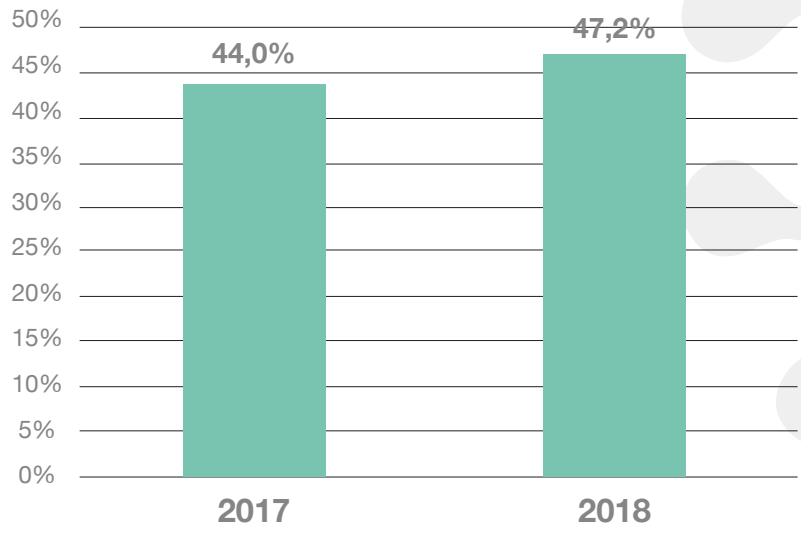


Gráfico 2. Porcentaje de elementos maliciosos detectados en ordenadores de sistemas de control industriales por anualidad, 2017 y 2018. Fuente: (Kaspersky Lab ICS CERT 2019).

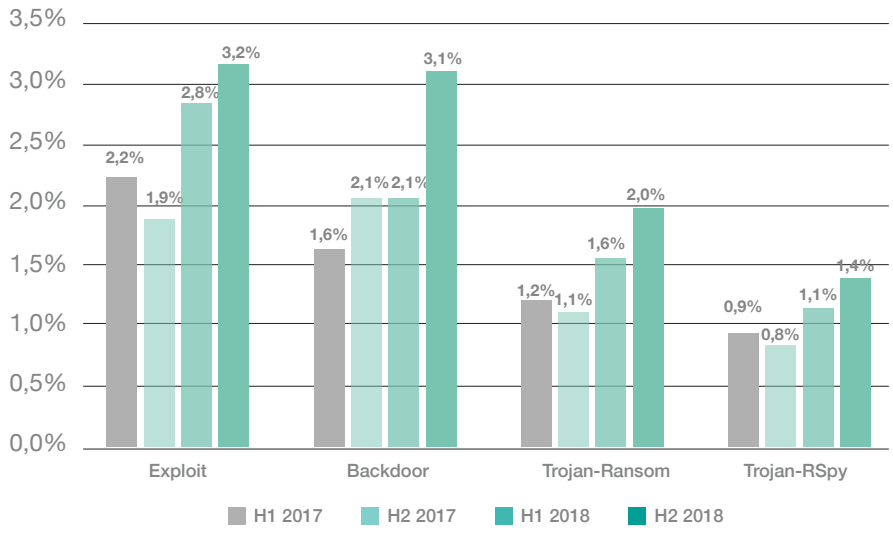


Gráfico 3. Porcentaje de elementos maliciosos detectados en ordenadores de sistemas de control industriales por el tipo de malware. Fuente: (Kaspersky Lab ICS CERT 2019).

En el trabajo de análisis realizado por el laboratorio de Kaspersky se detallan algunas estadísticas recientes sobre las amenazas en sistemas de control. El porcentaje de equipos en los que se detectaron objetos maliciosos creció en el año 2018 respecto del anterior hasta alcanzar un 47.2% (ver Gráfico 2). El troyano es el tipo *software* malicioso que predomina sobre el resto de amenazas en estos sistemas (ver Gráfico 3).

Por otra parte, las vulnerabilidades son debilidades en sistemas de información o control que pueden ser explotadas por una fuente de amenaza. Estas vulnerabilidades tienen diferentes orígenes, incluyendo un diseño inadecuado de la plataforma o dispositivo (*hardware* y/o *software*), fallos en su implementación, configuraciones erróneas, deficiente protección de las comunicaciones o carencias en las políticas y procedimientos.

El aumento de interés en este ámbito ha conllevado un aumento en la frecuencia de detección de vulnerabilidades, por lo que es importante revisar de forma continua las que afectan a los componentes de nuestro sistema. La infrecuente y, a menudo, difícil actualización de los elementos de un sistema de control abre la puerta al aprovechamiento de vulnerabilidades bien conocidas para las que incluso existen *exploits* de dominio público. Pero no basta con ello, ya que podemos encontrarnos también con vulnerabilidades de día cero, desconocidas hasta que son explotadas por un atacante. La longevidad de este tipo de sistemas también implica que nos encontremos con vulnerabilidades inherentes al diseño, como la utilización de protocolos inseguros, que no pueden ser resueltas y exigen la utilización de contramedidas adicionales.

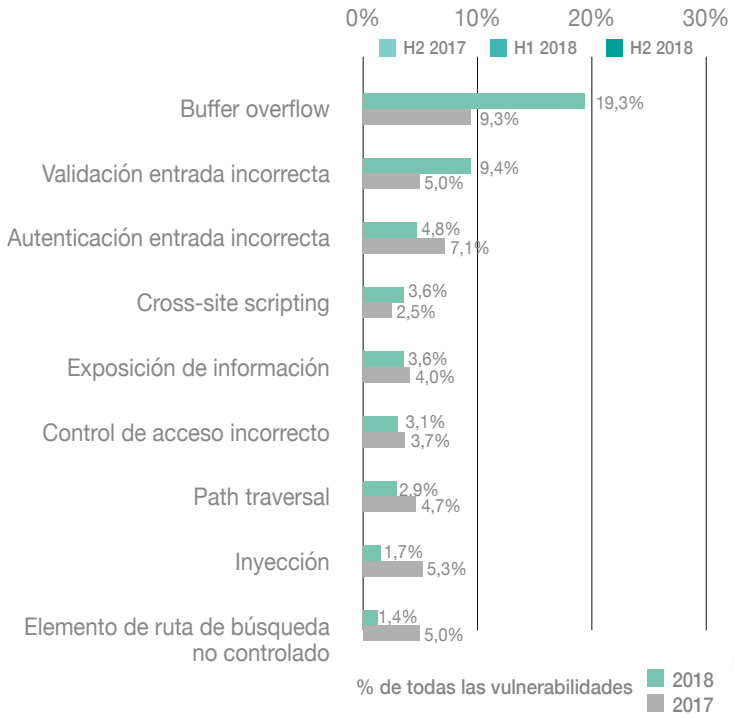


Gráfico 4. Tipos de vulnerabilidades detectadas en los años 2017 y 2018. Fuente: (Kaspersky Lab ICS CERT 2019)

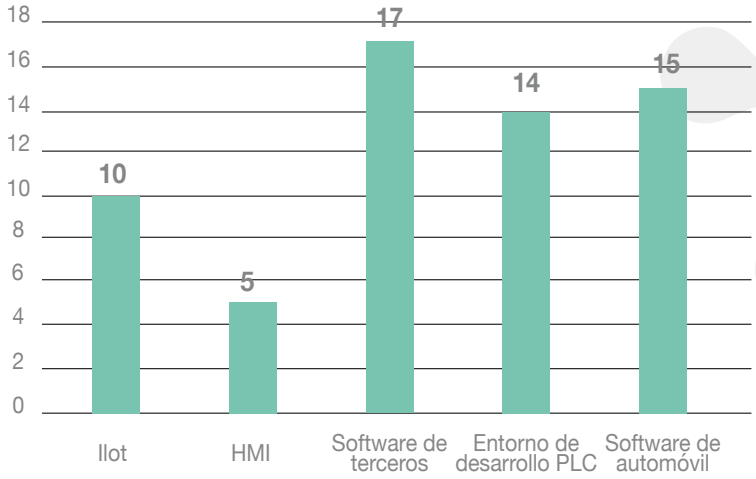


Gráfico 5. Número de detecciones por tipo de componente en 2018. Fuente: (Kaspersky Lab ICS CERT 2019)

Como ejemplo, en el Gráfico 4 se representa información sobre vulnerabilidades detectadas recientemente por el equipo Kaspersky. En la gráfica se muestra que, durante los años 2017 y 2018 la vulnerabilidad predominante fue el desbordamiento de *buffer*. En el Gráfico 5, se observa la distribución de las 29 vulnerabilidades reportadas a los fabricantes durante el año 2018 organizadas por elemento afectado. Puede observarse en dichos datos que no debe ignorarse la existencia de vulnerabilidades en ámbitos como los dispositivos de IoT o los automóviles.

Con respecto al dominio IoT, las vulnerabilidades se deben a menudo a los recursos limitados de los dispositivos, la urgencia de salida al mercado y la compleja distribución de actualizaciones. Estas vulnerabilidades pueden ser aprovechadas para la materialización de amenazas comunes a otros sistemas de control, u otras más específicas de estos sistemas como la falsificación del dispositivo o la interceptación de la sesión en un ecosistema complejo con servicios en la nube. En cuanto a los automóviles, vulnerabilidades en elementos como el sistema pasivo antirrobo utilizado en el arranque, los sistemas de apertura/cierre sin llave o las comunicaciones asociadas al sistema integrado de ocio (*Bluetooth*, telefónica, etc.), pueden ser utilizadas como vectores de ataque para comprometer las unidades electrónicas de control de algunas funciones críticas del coche como, por ejemplo, la dirección o los frenos.

El riesgo es una función de la probabilidad de que una amenaza suceda, por medio de aprovechamiento de una potencial vulnerabilidad de un recurso, con unas consecuencias en su funcionamiento. Puesto que podemos analizar la amenaza en cuanto a la fuente que la lleva a cabo, el vector de ataque que se utiliza para iniciarla y el objetivo, la reducción del riesgo deberá abordar estos tres elementos. Para evaluar las fuentes de amenaza es necesario a su vez considerar tres características: la capacidad de llevar a cabo un ataque, la intencionalidad de causar daño y la oportunidad de llevarla a cabo. Por otra parte, las consecuencias de un ataque en un sistema de control son potencialmente más graves que en otros sistemas de información, ya que manejan recursos físicos. Así, además de consecuencias económicas, legales o reputacionales comunes a otros sistemas, la pérdida de visualización, comunicación o control en un sistema de carácter industrial puede redundar en impactos verdaderamente graves y tangibles, como daños personales, al equipamiento y al medio ambiente.

El primer paso para una evaluación del riesgo es realizar una identificación de los recursos del sistema, de las amenazas potenciales para cada recurso, de las vulnerabilidades y de los controles de seguridad existentes. El examen de todo ello permitirá la determinación del impacto, la clasificación del riesgo y sugerirá controles de seguridad recomendables (Knapp and Langill, 2014).

- La caracterización del sistema mediante la identificación de los recursos es así el punto de partida. La recopilación de información, mediante la realización de un inventario, la lectura de documentación técnica, manuales o libros o el uso de herramientas de escaneo, será primordial para evaluar potenciales ataques.

- La identificación de amenazas potenciales para cada recurso es el paso más complicado, dado que hay que tener en cuenta la fuente de la amenaza, si es intencionada o no, interna o externa, así como los potenciales vectores de ataque, es decir, el método de acceso al objetivo como, por ejemplo, la explotación de servicios de red como el *e-mail* o la web,

dispositivos extraíbles, ingeniería social, etc. Es siempre útil mantenerse informado de incidentes, tendencias generales de ciberseguridad y conocer en profundidad el funcionamiento del sistema de control.

Los escáneres activos de vulnerabilidades, como OpenVAS o Tenable Nessus, son útiles para identificar vulnerabilidades existentes de un equipo comparándolas con aquellas conocidas e incluidas en su base de datos. También es útil mantenerse informado de nuevas vulnerabilidades detectadas en elementos del sistema de control mediante los avisos y alertas que envían los centros de respuesta temprana ante incidentes gubernamentales o del propio fabricante.

- La clasificación del riesgo proporciona una forma de evaluar las amenazas y vulnerabilidades identificadas. La última pieza de información relevante es una estimación de las consecuencias o impacto que produciría la materialización de la amenaza en la operatividad del sistema. Para ello, existen métodos cualitativos como el modelo DREAD, que permiten clasificar vulnerabilidades en diversas categorías (Knapp and Langill 2014), u otros que hacen uso de valores numéricos (Common Vulnerability Scoring System, CVSS). Para reducir los riesgos que superen un cierto umbral, será necesario aplicar controles de seguridad adicionales. Numerosas guías y normativa proporcionan recomendaciones útiles, que revisaremos posteriormente.

5. EJEMPLOS DE INCIDENTES

El estudio de incidentes previos no solamente es de gran utilidad para concienciar sobre la gravedad de los problemas de seguridad en los sistemas de control, sino también para comprender amenazas, malas prácticas, tendencias en el ámbito del cibercrimen o mecanismos de respuesta utilizados. A continuación, se realiza una breve descripción de algunos incidentes relevantes en instalaciones industriales o infraestructuras críticas.

STUXNET

Stuxnet es el ejemplo más emblemático de un ciberataque complejo contra una red industrial, ya que fue la primera vez que un *malware* era utilizado como un arma dirigida a dañar un sistema de control. Dicho *malware*, de una sofisticación inusual hasta la fecha, se cree que fue diseñado ex profeso para provocar daños en una planta nuclear iraní (Langner, 2011).

Aunque comenzó en 2007 su infección en sistemas, su descubrimiento no fue posible hasta 2010. La repercusión mediática de este incidente fue clave para que todos los agentes implicados en la seguridad industrial se concienciaran de su importancia. El *malware* fue capaz de infectar equipos basados en varias versiones del sistema operativo Windows, incluyendo cuatro vulnerabilidades de día cero.

El objetivo principal era la inyección de código malicioso a PLCs S7 de Siemens, cuya estrategia de control tuviese unas características muy determinadas; concretamente, que contase con una configuración determinada de variadores que se encuentran en automatizaciones de centrifugadoras de

uranio. Mediante el aprovechamiento de vulnerabilidades en el *software* de programación STEP7 y en SCADA SIMATIC WinCC, realizaba modificaciones frecuentes de las velocidades de giro de los motores, ocultando este hecho a los operadores. Si el equipo no tenía la configuración deseada, el *malware* permanecía oculto. Además, contaba con sofisticadas formas de propagarse.

Este incidente es el primer ejemplo de amenaza persistente avanzada dirigida a una red industrial, que aprovecha vulnerabilidades de políticas y procedimientos -como el control insuficiente de la conexión de medios externos-, de *software* de uso general y, lo que es más interesante, de *software* específico de automatización.

DRAGONFLY/HAVEX

Hablamos de las campañas de espionaje en Estados Unidos y Europa, especialmente en el sector eléctrico y petroquímico, que utilizaron técnicas como *spear phishing* y *watering hole* como vectores y un troyano de acceso remoto descubierto en 2014 conocido como Havex. Dicho *malware* despliega funcionalidades nunca vistas anteriormente, como la utilización de OPC para obtener información de los recursos compartidos en la red. Es de interés como ejemplo por tratarse del primer caso de aprovechamiento de protocolos industriales.

RED ELÉCTRICA UCRANIANA

Sabotaje coordinado a la red eléctrica ucraniana en diciembre de 2015, que afectó a 30 subestaciones y 225.000 personas durante 6 horas (Hemsley and Fisher, 2018). En este ataque se hizo uso de BlackEnergy, un *malware* utilizado desde 2007 en ataques de denegación de servicio, del que ha habido diversas versiones. No obstante, aunque el *malware* permitió el ataque y retrasó la restauración de los sistemas, la interrupción del servicio fue provocada por la acción directa y coordinada de los atacantes. Así, tras haber obtenido credenciales e información sobre la infraestructura por medio de *spear phising* con archivos de Excel, los atacantes fueron capaces de realizar conexiones mediante VPN y escritorios remotos.

Durante el ataque coordinado, enviaron comandos desde el *software* de supervisión, inyectaron *firmware* corrupto en dispositivos de comunicaciones, manipularon los SAIs, utilizaron el *malware* KillDisk para el borrado de discos y realizaron un ataque de denegación al servicio de atención telefónica. Este incidente es otro ejemplo de amenaza persistente avanzada que se caracteriza por un aprovechamiento conjunto y coordinado de varias vulnerabilidades y cuyo objetivo es maximizar el tiempo de interrupción del servicio.

INDUSTROYER/CRASHOVERRIDE

Fue un ciberataque ocurrido, de nuevo, en la red eléctrica ucraniana a finales de 2016, aunque no tuvo tanto impacto. En este caso se hizo uso de un *malware* específicamente diseñado para atacar redes eléctricas, que muestra un nivel de evolución nunca visto anteriormente, ya que se trata de

una plataforma enteramente orientada a realizar ataques contra sistemas de la red de distribución eléctrica, sin limitarse a una plataforma específica de un fabricante -como ocurría con Stuxnet- o al espionaje -como Havex- (Cherepanov, 2017).

Dicho *malware* explota librerías y ficheros de configuración de HMIs para conocer mejor su entorno y poder pivotar desde ahí. Adicionalmente, cuenta con módulos para OPC DA, IEC 60870-5-101/14 e IEC 61850, que permiten enumerar elementos y, en algunos casos, enviar órdenes. También cuenta con una herramienta de denegación de servicio de relés de protección de Siemens y un componente de borrado de datos. Este incidente muestra la tendencia a aprovechar diferentes vulnerabilidades para diversificar los ataques y evidencia que los atacantes pueden contar numerosos recursos y amplios conocimientos.

TRITON/TRISIS/HATMAN

Se trata de un *malware* descubierto inicialmente en 2017, cuyo objetivo eran los sistemas instrumentados de seguridad Triconex de Schneider Electric, intentando modificar el *firmware* para añadir programación adicional y comunicando mediante el protocolo propietario que utilizan dichos sistemas. Se cree que fue introducido en la red de seguridad operacional mediante ingeniería social. Posteriormente, se utilizaron dos usuarios privilegiados no documentados que permitían exponer información sobre la compilación.

Afortunadamente, el *malware* no tuvo el efecto deseado, porque los controladores iniciaron un estado seguro que provocó una parada del proceso. No obstante, este incidente pone de manifiesto que ni los SIS, generalmente aislados del resto del sistema de control, están a salvo de posibles ataques. Esto es especialmente grave, puesto que estos sistemas tienen la capacidad de tomar el control y llevar al sistema a una parada de emergencia que puede tener consecuencias físicas si no se lleva a cabo de forma ordenada. También sirve como ejemplo de vulnerabilidades potenciales en los dispositivos -como usuarios no documentados o *firmware* no cifrado- o debidas a un uso incorrecto por parte del personal de planta, que desconocía medidas básicas de seguridad del dispositivo.

BOTNETS DE DISPOSITIVOS IOT

En los últimos años se han repetido incidentes en diferentes dispositivos encuadrables en la Internet de las Cosas de carácter doméstico que han sido utilizados en denegaciones de servicio distribuidas. Aunque aún no se conocen incidentes importantes que utilicen dispositivos de un carácter industrial, esta tendencia pone de manifiesto que las vulnerabilidades de diseño e implementación pueden convertir a los dispositivos IoT en una herramienta para realizar ataques sobre otros objetivos.

El ejemplo más conocido es el de Mirai, un *malware* orientado a crear y controlar una botnet -red de dispositivos utilizados remotamente por un atacante- para realizar denegaciones de servicio masivas, las cuales alcanzaron 1,5 Tbps. Estos incidentes ponen de manifiesto que la multiplicación de dispositivos de bajo coste con conexión de red aumenta la superficie de ataque y dificulta su protección.

6. INICIATIVAS Y ESTÁNDARES

6.1. ORGANIZACIONES Y ENTIDADES RELACIONADAS

Varias entidades relevantes pueden servir como fuentes de información en este ámbito: instituciones gubernamentales, organizaciones desarrolladoras de normativa, asociaciones y centros especializados en este campo. En la tabla siguiente se resumen varias de las organizaciones y entidades desarrolladoras de normativa relacionada con los sectores estratégicos.

Tabla 1 Organizaciones y entidades desarrolladoras de normativa. Fuente: propia.

	Nombre	Tipo
ISO	International Organization for Standardization	Internacional
IEC	International Electrotechnical Commission	Internacional
IEEE-SA	IEEE- Standards Association	Internacional
ITU-T	International Telecommunication Union-Telecomm. Sector	Internacional
CEN	European Commitee for Standardization	Europa
ETSI	European Telecommunications Standards Institute	Europa
CENELEC	Comité Européen de Normalisation Electrotechnique	Europa
NIST	National Institute of Standards and Technology	Norteamérica
ANSI	American National Standards Institute	Norteamérica
NERC	North American Electric Reliability Corporation	Norteamérica
NRC	United States Nuclear Regulatory Commission	Norteamérica
AGA	American Gas Association	Norteamérica
API	American Petroleum Institute	Norteamérica
CFATS	Chemical Facility Anti-Terrorism Standards	Norteamérica
CISA	Cybersecurity and Infrastructure Security Agency	Norteamérica
ENISA	EU Agency for Network and Information Security	Europa
ENCS	European Network for Cyber Security	Europa
INCIBE	Instituto Nacional de Ciberseguridad	España
CNPIC	Centro Nacional de Protección de Infraestructuras Críticas	España
CCI	Centro de Ciberseguridad Industrial	España
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information	Francia

La protección de las infraestructuras críticas ha sido un asunto de gran preocupación mundial, resultando en legislaciones a nivel internacional y estatal. En el ámbito europeo, la legislación comenzó inicialmente con comunicaciones como, por ejemplo, la 702 del 20 de octubre de 2004 sobre Protección de las infraestructuras críticas en la lucha contra el terrorismo, el Libro Verde en 2005 sobre el Programa europeo de protección de infraestructuras críticas (PEPIC) o, más tarde, el Programa europeo para la protección de infraestructuras críticas [COM (2006) 786], que estableció los instrumentos para llevar a la práctica el PEPIC. Posteriormente se introdujo la Directiva 2008/114/CE, que establece criterios de identificación y designación de infraestructuras críticas europeas y el planteamiento común para evaluar la necesidad de mejorar su protección.

Como consecuencia de dicha actividad, se creó en España el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) en 2007. Este centro es un órgano coordinador para el procedimiento del Esquema de Planificación PIC, basado en la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y el Real Decreto 704/2011 de 20 de mayo, que aprueba el Reglamento PIC, y definen las medidas necesarias para garantizar la protección de las infraestructuras críticas. Para ello, se utilizan una serie de instrumentos:

- De carácter estratégico y responsabilidad del Estado
  - *Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC)*, dirigido a mantener seguras las infraestructuras españolas que proporcionan los servicios esenciales a la sociedad.
  - *Planes Estratégicos Sectoriales (PES)* para cada uno de los sectores contemplados por la ley.
- De responsabilidad del titular de la infraestructura crítica:
  - *Planes de Seguridad del Operador (PSO)*, documentos estratégicos que definen las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones de su gestión.
  - *Planes de Protección Específicos (PPE)*, documentos operativos donde se definen medidas concretas para garantizar la seguridad integral (física y lógica) de sus infraestructuras críticas.
- De carácter operativo y responsabilidad de fuerzas y cuerpos de seguridad
  - *Planes de Apoyo Operativo (PAO)*, con medidas concretas en apoyo de los operadores de infraestructuras críticas.

6.2. EQUIPOS DE RESPUESTA

Un Equipo de Respuesta ante Emergencias Informáticas (*Computer Emergency Response Team*, CERT) es un grupo de personas dedicado al desarrollo de medidas preventivas y reactivas ante ataques a la seguridad de los sistemas de información. Con el paso del tiempo, sus servicios han ido evolucionando desde la gestión de incidentes hacia un modelo integral de gestión de la seguridad y actualmente juegan un papel imprescindible en un mundo conectado con permanentes ciberataques.

Existen numerosos CERTs, varios incluso dentro de un mismo país. En España cabe destacar INCIBE-CERT que, en lo relativo a la gestión de incidentes de operadores críticos del sector privado, es operado conjuntamente por INCIBE y CNPIC, y el CCN-CERT del Centro Criptológico Nacional.

A nivel internacional, también es interesante reseñar la Agencia de Seguridad de Infraestructura y Ciberseguridad estadounidense (CISA), que integra el antiguo ICS-CERT, que ha sido históricamente la mayor referencia en el ámbito de la ciberseguridad de los sistemas de control industriales.

La coordinación de estos equipos es primordial para que su labor sea eficaz, incluso hay organizaciones que facilitan esta tarea, entre las que cabe destacar, a nivel europeo, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

6.3. ESTÁNDARES, NORMAS Y GUÍAS

Existen normas, estándares y guías orientadas a una diversa audiencia que va desde proveedores de sistemas de control hasta usuarios finales. En general, cubren requisitos generales para aplicar la seguridad, pero no tienen en cuenta las particularidades específicas de una determinada instalación industrial. Por tanto, cada recomendación o regla incluida en la normativa debe considerarse teniendo en cuenta el entorno industrial al que se va a aplicar.

El estándar ISA/IEC-62443 es el más importante en cuanto a la seguridad industrial. Parte originalmente del ISA-99, más tarde fue publicado como ANSI/ISA-62443 y finalmente fue elevado a estándar internacional IEC-62443. Consiste en una serie de normas de ciberseguridad industrial que definen procedimientos para su implementación segura en la automatización industrial y los sistemas de control. Está dirigida no sólo a fabricantes, sino también a usuarios, profesionales y académicos/as. Por otra parte, el conjunto de normas ISO/IEC 27000 contiene las mejores prácticas recomendadas para el mantenimiento de sistemas de gestión de la seguridad de la información (SGSI). La ISO/IEC 15408, referida como *Common Criteria*, establece un proceso de criterios de evaluación para la seguridad de productos *software*.

La combinación de IEC 61968 e IEC 61970 forman el *Common Information Model* (CIM) y permite que aplicaciones informáticas intercambien información sobre una red eléctrica. La norma IEC 61970-301 describe componentes de un sistema eléctrico, mientras que la IEC 61968-11 cubre otros aspectos para el *software* como la gestión de activos y sistemas de información al cliente. La norma IEC-62351 desarrolla normas de ciberseguridad para protocolos de comunicación en sistemas de potencia. Entre las familias de normas realizadas por el IEEE también conviene reseñar: IEEE P1711 (IEEE Standard for a Cryptographic Protocol for EPS Serial Links); IEEE 1402 (IEEE Guide for Electric Power Substation Physical and Electronic Security) y IEEE 1686 (IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities).

La North American Electric Reliability Corporation (NERC) publicó un conjunto de estándares (NERC-CIP, Critical Infrastructure Protection) de obligatorio cumplimiento en Estados Unidos para asegurar la operación de un sistema de generación y transporte eléctrico. NERC CIP cubre la seguridad de activos críticos, la formación de personal, la gestión de la seguridad y las estrategias de respuesta ante incidentes. Por otra parte, la serie de documentos AGA12 propone prácticas di-

señadas para la protección criptográfica de las comunicaciones Finalmente, el NIST Cybersecurity Framework, desarrollado en Estados Unidos, proporciona unas guías de ayuda a organizaciones y sectores críticos, entre las que destacan las referidas a sistemas de control:

NIST Special Publication 800-82: Guide to industrial control systems (ICS) security, mayo de 2015.

NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations, abril de 2013.

7. RECOMENDACIONES DE SEGURIDAD INDUSTRIAL

Muchas son las prácticas de seguridad requeridas y/o recomendadas por las organizaciones y fabricantes. A continuación, se mencionan buenas prácticas que son comunes y forman una base mínima. Estas prácticas se integran en una estrategia de defensa en profundidad, es decir, en la combinación en capas de diferentes mecanismos de seguridad que, al complementarse entre sí, permiten mejorar la protección. Dicha estrategia ha de considerar la seguridad en varios contextos debido a la segregación existente en áreas industriales:

- La capa física, incluyendo el control de acceso de personal autorizado a las zonas, paneles, dispositivos y salas de control por medio de llaves, tarjetas, dispositivos biométricos, etc.

- La capa de red, haciendo uso de sistemas de detección y prevención tanto en el perímetro como en la protección interna de las redes y de la comunicación entre las mismas.

- Los dispositivos, que en este caso son altamente heterogéneos, debiendo considerar la actualización de los mismos, la limitación de servicios activos a los estrictamente necesarios, la utilización de elementos pasivos o activos de protección, etc.

- Los datos y aplicaciones, mediante el uso de mecanismos de autenticación y autorización centrados en el principio del menor privilegio, contraseñas fuertes, etc.

- Los procedimientos y políticas, entre los que se encuentran los de gestión de recursos y cambios, respuesta ante incidentes, de formación, etc.

Su gestión es necesariamente cíclica para poder adaptarse y requiere de la implicación, en mayor o menor medida, de todo el personal. Es, por tanto, conveniente que exista la concienciación y formación suficiente para que la seguridad sea un factor a considerar en todas las decisiones.

7.1. IDENTIFICACIÓN DE SISTEMAS CRÍTICOS

El primer paso para asegurar un sistema es la identificación de lo que necesita protegerse, que no siempre es una tarea sencilla. Es necesario realizar un completo inventario de los dispositivos conectados, los cuales deberían evaluarse independientemente si realizan una actividad crítica o están conectados a alguna.

La normativa NERC CIP de las compañías eléctricas de Norte América proporciona un proceso para identificar recursos y separarlos en críticos y no críticos, incluyendo también un determinado grado de criticidad que ayude a su priorización.

7.2. SEGURIDAD DE RED

Se recomienda la separación de activos lógicos y físicos en grupos (o zonas) que comparten requisitos de seguridad comunes, lo cual permite identificar los flujos de información entrantes y salientes -que también se pueden agrupar en conductos- y así establecer el nivel de seguridad disponible. La comparación de este nivel de seguridad con el deseado sugerirá las medidas de protección adicionales que deben establecerse dentro de cada grupo o entre ellos (Knapp and Langill, 2014).

Importantes fuentes de recomendación como el estándar IEC/ISA 62443 hacen mucho énfasis en este proceso, proponiendo modelos para la creación de grupos funcionales y la evaluación de riesgos. En el terreno industrial este método se puede utilizar porque la red se suele mantener estable a lo largo del tiempo y las funciones de cada elemento están bien definidas.

Una de las medidas más importantes para materializar la estrategia anterior es la segmentación de red, que separa las redes en otras más pequeñas y manejables, de acuerdo a las agrupaciones definidas. Esta segmentación puede ser implementada en los niveles de red o superiores mediante listas de control de acceso, cortafuegos de sesión o con filtrado a nivel de aplicación; en la capa de enlace, mediante redes locales virtuales; o a nivel físico, mediante diodos de datos.

Por otra parte, es necesario reforzar la seguridad perimetral, limitando los accesos externos a las redes industriales a su mínima expresión y haciendo uso de mecanismos como las redes privadas virtuales o el establecimiento de lo que en seguridad informática se conoce como zonas desmilitarizadas. También es necesario deshabilitar la utilización de dispositivos extraíbles y móviles.

7.3. CONTROL DE ACCESO A DATOS Y APLICACIONES

Existen diversos principios a considerar a la hora de gestionar el acceso a datos o aplicaciones. Los más importantes son la separación de responsabilidades, el mínimo privilegio, la identificación unívoca y la supervisión continua de la actividad.

Es necesario también asegurar buenas prácticas de autenticación y autorización, que pueden incluir mecanismos multi-factor, biométricos, basados en *tokens* físicos, etc. Las credenciales o contraseñas han de ser gestionadas adecuadamente. La implementación adecuada de las tecnologías disponibles para este propósito no es trivial y, de nuevo, la aplicación de varias capas de complejidad contribuye a una mayor protección. Por ejemplo, es conveniente combinar credenciales con operaciones limitadas a un área o turno de operación, limitando la autorización de las operaciones a aquellos usuarios con la autoridad necesaria que acceden desde un dispositivo del grupo funcional requerido.

7.4. SEGURIDAD DE LOS EQUIPOS

En lo relativo a la seguridad de los equipos, el primer paso es el bastionado del sistema, es decir, el bloqueo de todos los servicios innecesarios para su actividad, limitando así la superficie de ataque. El uso de herramientas de supervisión del sistema en dispositivos de control y equipos de supervisión, incluyendo los destinados a vigilar la integridad o filtración de los ficheros y aquellos orientados a la detección de intrusiones (*Host* IDSs) o firmas de *malware* conocido (antivirus), estará limitado, pese a su utilidad, por la capacidad computacional y la necesidad de garantizar la disponibilidad. Es por ello que, a menudo, se recurre a una política de listas blancas que definen las aplicaciones y ficheros permitidos y bloquean todo lo demás, lo que es factible puesto que los sistemas de control se mantienen sin apenas cambios a lo largo de su ciclo de vida.

La gestión de las actualizaciones es compleja porque la utilización de herramientas automáticas no suele ser posible. Por otra parte, parchear sobre sistemas en producción es inaceptable y mantener un entorno de réplica es caro, por lo que, generalmente, se necesitará planificar las actualizaciones durante las paradas previstas del sistema. En esta línea, es clave mantenerse informado de las vulnerabilidades y parches para comprender las medidas de protección alternativas que podríamos necesitar para asegurar los sistemas no actualizados. No obstante, para la gestión de estas vulnerabilidades no se deberían utilizar herramientas de descubrimiento activas que puedan perturbar el comportamiento normal del sistema. Para la aplicación de cualquiera de las medidas anteriores, existe una gran dependencia del fabricante, por lo que una gestión adecuada de la documentación facilitará mucho este proceso.

7.5. SUPERVISIÓN DE LA SEGURIDAD

La monitorización de eventos mediante sistemas de detección de intrusiones en red (IDS, de sus siglas en inglés *Intrusion Detection System*) es apropiada en todas las zonas de interés porque se trata de una solución no intrusiva. Esta detección puede estar basada en firmas o en la detección de anomalías con respecto a un modelo base de tráfico de red normal (Axelsson 2000).

La correlación de la información obtenida a partir del tráfico de red y del registro de eventos detectados a nivel de equipo en los elementos del sistema de control puede facilitar tanto la respuesta ante incidentes, como su posterior auditoría y documentación. Para ello, existen unos sistemas conocidos como correladores de eventos o Sistemas de Información de Seguridad y Gestión de

Eventos (SIEM, *Security Information and Event Management*) que facilitan la visualización y filtrado de información para que un experto en seguridad pueda buscar síntomas típicos de un incidente. En el caso que nos ocupa, la información del proceso industrial también podría resultar útil para proporcionar un contexto que facilite la interpretación.

7.6. OTRAS RECOMENDACIONES

También existen recomendaciones específicas para cada elemento. Por ejemplo, en el puesto de ingeniería es muy importante conservar un registro de todos los eventos y garantizar la autenticidad e integridad de la configuración y las comunicaciones, mientras que en los dispositivos de control se debería firmar el *firmware*, almacenar de forma segura la información confidencial y controlar las interfaces físicas de acceso.

Dado el campo de continuo desarrollo que es la ciberseguridad y la inmadurez en el entorno industrial, surgen continuamente nuevos productos y tecnologías que implementan protecciones de seguridad adicionales. Por tanto, un buen ejercicio es revisar continuamente la tecnología disponible.

8. FORMACIÓN Y EXPERIMENTACIÓN

La formación de profesionales en el ámbito de la ciberseguridad industrial es verdaderamente relevante puesto que todos los informes señalan la escasez de estos perfiles en el mercado a nivel internacional. Es necesario, por tanto, acercar dos perfiles tradicionalmente muy diferenciados como son los expertos en automatización y los especialistas en seguridad. Entre las recomendaciones generales que podemos encontrar en la literatura con respecto a la formación en ciberseguridad industrial, las más interesantes son las del informe de la francesa *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI), que plantea un sistema de formación modular que se ajuste a diferentes perfiles.

En los últimos años, ha aumentado considerablemente la oferta de cursos de especialización en este ámbito con una naturaleza profesional. Por otra parte, aunque no es frecuente encontrar asignaturas centradas en este tema en programas de posgrado en ciberseguridad impartidos por universidades españolas debido a la disparidad de objetivos y orientaciones de dichos másteres, sí que están disponibles, al menos, en las universidades de Cádiz, León, Politècnica de Catalunya y la de Valencia.

Uno de los principales retos en la formación práctica es que muchas veces ésta se centra bien en la gestión aislada de dispositivos industriales o de red, bien en simulaciones, lo que proporciona a los estudiantes una comprensión limitada del problema, especialmente a aquellos que provienen del mundo de las tecnologías de la información. Por eso, es interesante contar con sistemas de experimentación más completos.

Con respecto a la investigación, dada la dificultad para realizar evaluaciones de seguridad de un sistema de control en producción, también es necesario contar con bancos de pruebas en los cuales se pueda realizar experimentación de manera segura. Sin embargo, muchos de los creados

hasta el momento se basan en simulaciones, un enfoque de bajo coste del que se pueden destacar ejemplos como SCADASim (Queiroz, Mahmood, and Tari, 2011), que proporciona un marco de trabajo modular que simula dispositivos y redes para estudiar ataques en ellos, o SCADA-SST (Ghaleb, Zhioua, and Almulhem, 2016), que presenta un entorno de simulación sencillo de configurar para pruebas de seguridad soportando varias arquitecturas. Con todo, este enfoque no replica con fidelidad las situaciones que se producen en la realidad, puesto que no pueden simular todas las interacciones que ocurren en los sistemas de control ni las características específicas de una tecnología o implementación en cada uno de los elementos del sistema.

Otro enfoque, el de la virtualización, aporta nuevas formas de integrar elementos físicos con *software*. Por ejemplo, la plataforma virtual propuesta por Reaves y Morris (2012) simula entornos con varios protocolos de comunicación. Otro ejemplo es SCADAVT (Almalawi et al., 2013), que construye un banco de pruebas basado en un emulador CORE incluyendo los componentes esenciales de un sistema de control.

Por otra parte, los laboratorios que incorporan equipos *hardware* son más costosos y complejos de desarrollar, pero proporcionan resultados más fiables. La creación de bancos de pruebas con similares características a las estructuras reales permite una gran flexibilidad en cuanto a los experimentos o actividades que pueden llevarse a cabo sobre él: el análisis de vulnerabilidades y técnicas de ataque que afectan a los sistemas de control y sus protocolos de comunicaciones, validación experimental de amenazas y la implementación de contramedidas, programas de formación y concienciación de profesionales. Un buen ejemplo de banco de pruebas realista es el propuesto por Candell et al. (2015), diseñado para demostrar la seguridad en varios procesos aplicando la normativa NIST SP 800-82 y medir su rendimiento.

En este sentido, también se ha desarrollado en la Universidad de León un laboratorio de ciberseguridad de infraestructuras críticas (CICLab) (Domínguez et al., 2017), cubriendo cuatro áreas principales: sistemas de control industriales, sistemas de suministro eléctrico, gestión de edificios y redes inalámbricas. Dicho laboratorio resguarda al menos los tres niveles inferiores de la pirámide de automatización en cada caso y está diseñado para ofrecer flexibilidad en cuanto a la arquitectura del sistema de control, conectividad de la red y medidas de seguridad activas. Para ello, en la parte puramente informática, se hace uso de virtualización, que conjuntamente con equipamiento industrial, de comunicaciones y de seguridad real, equivalente al encontrado en automatizaciones de infraestructuras críticas, permite a un investigador o investigadora diseñar la estructura que más se ajuste a sus necesidades.

Otra característica de este laboratorio es el objetivo de abarcar el mayor número posible de tecnologías. Por ello, el sistema de control industrial se compone de tres anillos de automatización: uno principal (con comunicación Modbus TCP o Ethernet/IP) y dos anillos secundarios, en los cuales se incluyen dispositivos esclavos y pasarelas de comunicación para diferentes tipos de redes. En el sistema de gestión de edificios se incluyen diferentes redes, como LonWorks, BACnet o KNX, así como comunicaciones inalámbricas basadas en las especificaciones ZigBee y EnOcean. Las arquitecturas del sistema eléctrico siguen similares características a las encontradas en subestaciones, incluyendo unidades centrales, dispositivos de control, protección y medida, etc. También dispositivos situados en el cliente, como contadores inteligentes.

9. CONCLUSIONES

La digitalización de la industria ha llevado a la integración de tecnologías de información y operación, aportando numerosas ventajas en los procesos productivos. Sin embargo, dispositivos que tradicionalmente se entendieron aislados se ven expuestos actualmente a amenazas que pueden llevar a graves consecuencias. Esto es especialmente cierto para los sistemas de control que pueden encontrarse en las infraestructuras críticas.

Por ello, en este capítulo se ha realizado una breve revisión de los sistemas industriales desde el punto de vista de su seguridad, prestando especial atención a las amenazas y vulnerabilidades asociadas a ellos. Se han revisado incidentes previos, así como las organizaciones y entidades relevantes que han redactado la normativa y estándares de aplicación. Finalmente, se han sintetizado las recomendaciones de seguridad más habituales en este ámbito, haciendo énfasis en las particularidades que diferencian a los sistemas de control de otros sistemas de información. También se ha reflexionado sobre las actividades de experimentación y formación, que son cada día más importantes para alcanzar un nivel de concienciación y madurez semejante al conseguido en otros ámbitos de la ciberseguridad.

10. BIBLIOGRAFÍA

Alcaraz, Cristina, and Sherali Zeadally (2015). Critical Infrastructure Protection: Requirements and Challenges for the 21st Century. *International Journal of Critical Infrastructure Protection 8*, 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002

Almalawi, Abdulmohsen, Zahir Tari, Ibrahim Khalil, and Adil Fahad (2013). SCADAVT-A Framework for Scada Security Testbed Based on Virtualization Technology. In *Local Computer Networks (Lcn), 2013 IEEE 38th Conference on*, 639–646.https://doi.org/ 10.1109/LCN.2013.6761301

Agence Nationale de la Sécurité des Systèmes D'Information (ANSSI) (2015). *Guide Pour Une Formation Sur La Cybersécurité Des Systèmes Industriels*. https://www.ssi.gouv.fr/uploads/2015/03/Guide_pour_une_formation_sur_la_cybers%C3%A9curit%C3%A9_des_syst%C3%A8mes_industriels.pdf

Axelsson, Stefan (2000). *Intrusion Detection Systems: A Survey and Taxonomy*. Technical report. https://www.researchgate.net/publication/2597023_Intrusion_Detection_Systems_A_Survey_and_Taxonomy

Candell, Richard, Timothy Zimmerman and Keith Stouffer (2015). *An Industrial Control System Cybersecurity Performance Testbed*. National Institute of Standards and Technology. NIST Interagency/Internal Report (NISTIR) - 8089. https://doi.org/10.6028/NIST.IR.8089

Cardenas, Alvaro, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, Shankar Sastry et al. (2009). Challenges for Securing Cyber Physical Systems. Workshop on Future Directions in Cyber-physical Systems Security, DHS (23 de julio de 2009). https://ptolemy.berkeley.edu/projects/chess/pubs/601/cps-security-challenges.pdf

Cherepanov, Anton (2017). Win32/Industroyer: A New Threat for Industrial Control Systems. White Paper, ESET. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Da Xu, Li, Wu He, and Shancang Li (2014). internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics* 10 (4). IEEE: 2233–43. https://doi.org/10.1109/TII.2014.2300753

Domínguez, Manuel, Miguel A., Prada, Perfecto, Reguera, Juan, J Fuertes, Serafín Alonso, and Morán, Antonio (2017). Cybersecurity Training in Control Systems Using Real Equipment. *IFAC-PapersOnLine* 50 (1). Elsevier: 12179–84. https://doi.org/10.1016/j.ifacol.2017.08.2151

Ghaleb, Asem, Sami, Zhioua, and Ahmad, Almulhem. 2016. SCADA-SST: A SCADA Security Testbed. In Industrial Control Systems Security (WCICSS), 2016 World Congress on, 1–6. IEEE. https://doi.org/10.1109/WCICSS.2016.7882610

Hemsley, Kevin, and Fisher, Ronald (2018). A History of Cyber Incidents and Threats Involving Industrial Control Systems. Staggs J., Shenoi S. (eds) *Critical Infrastructure Protection XII*. ICCIP 2018. IFIP Advances in Information and Communication Technology, 542. Springer, Cham.

Kaspersky Lab ICS CERT. 2019. *Threat Landscape for Industrial Automation Systems H2 2018*. https://ics-cert.kaspersky.com/media/KL_ICS_CERT_H2_2018_REPORT_EN.pdf

Knapp, Eric D, and Thomas Langill, Joel (2014). *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, Scada, and Other Industrial Control Systems*. Amsterdam: Syngress.

Langner, Ralph. 2011. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy* 9 (3). IEEE: 49–51. https://doi.org/10.1109/MSP.2011.67

Lee, Edward A. (2008) Cyber Physical Systems: Design Challenges. In *2008 11th Ieee International Symposium on Object and Component-Oriented Real-Time Distributed Computing (Isorc)*, 363–69. IEEE. https://www2.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.pdf

Lee, Jay, Bagheri, Behrad and Kao, Hung-An (2015). A Cyber-Physical Systems Architecture for Industry 4.0-Based Manufacturing Systems. *Manufacturing Letters 3*. Amsterdam: Elsevier, 18–23. https://doi.org/10.1016/j.mfglet.2014.12.001

Lu, Yang (2017) Industry 4.0: A Survey on Technologies, Applications and Open Research Issues. *Journal of Industrial Information Integration*, 6, 1–10. https://doi.org10.1016/j.jii.2017.04.005

Mandado-Pérez, Enrique, Marcos-Acevedo, Jorge and Fernández-Silva, Celso (2009) *Autómatas Programables y Sistemas de Automatización*. Barcelona: Marcombo.

Queiroz, Carlos, Mahmood, Abdun and Tari, Zahir (2011). SCADASim—A Framework for Building SCADA Simulations. *IEEE Transactions on Smart Grid 2* (4). IEEE: 589–97.

Reaves, Bradley and Morris, Thomas (2012). An Open Virtual Testbed for Industrial Control System Security Research. *International Journal of Information Security 11* (4), 215–29. https://doi.org/10.1007/s10207-012-0164-7

Rinaldi, Steven M, Peerenboom, James P. and Kelly, Terrence (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine 21* (6), 11–25. https://doi.org/10.1109/37.969131

Sisinni, Emiliano, Song Han, Abusayeed Saifullah, Jennehag, Ulf and Gidlund, Mikael (2018) Industrial internet of Things: Challenges, Opportunities, and Directions. *IEEE Transactions on Industrial Informatics 14* (11), 4724–4734. https://doi.org/10.1109/TII.2018.2852491

Stouffer, Keith et al (2015). NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security. *NIST*. http://dx.doi.org/10.6028/NIST.SP.800-82r2

CAPÍTULO IV

INVESTIGACIÓN Y ANÁLISIS FORENSE TECNOLÓGICO

IV. Investigación y análisis forense tecnológico

Por Javier Marqués y José Torres

** Javier Marqués es Profesor de FP en el CIPFP Luis Súñer Sanchís de Alzira. Perito e ingeniero en Telemática y Socio Gerente del Instituto Valenciano de Ciberseguridad y Telemática (INVACI).*

** José Torres es vicedirector de la Escola Tècnica Superior d'Engingeria (ETSE) de la Universitat de València y profesor titular del departamento de Ingeniería Electrónica.*

1. INTRODUCCIÓN

Las técnicas y motivaciones de ataque y penetración son diferentes en cada sistema al tiempo que surgen nuevas, cada hora, cada minuto y cada segundo. Esta situación supone una dificultad creciente para los especialistas en ciberseguridad a la hora de investigar y estudiar estos ataques.

Por ello, dentro de la informática y de las telecomunicaciones, o más concretamente, dentro de la telemática, existe un espacio dedicado al estudio y la investigación de los entornos en los que se ha producido alguna acción ilegal o no consensuada. Surge la necesidad de crear herramientas, estrategias y acciones que permitan descubrir, en un entorno tecnológico, la evidencia digital que sustente y verifique los hechos delictivos o no consentidos que se han producido.

La investigación y el análisis forense tecnológico intentan dar respuesta a los problemas de ciberseguridad, y se centran en recolectar y utilizar la evidencia digital en casos de delitos informáticos y telemáticos. Un o una forense tecnológico hace uso de todas las herramientas y conocimientos disponibles a su alcance para poder descubrir las evidencias digitales en un disco duro, en una memoria extraíble, en un archivo, en un correo electrónico, en un *smartphone*, en una red de datos o en un *router*.

La correcta realización de un análisis forense nunca debe realizarse sin previamente haber llevado a cabo una investigación y un estudio minucioso, ya que correríamos el riesgo de eliminar evidencias digitales. Una vez que el sistema ha sido atacado, entre otras cosas, va a proporcionar una recreación del incidente, permitiendo diseñar un proceso de corrección segura. También debe permitirnos conocer que provocó la intrusión, de modo que podamos evitar que se repita la misma situación de riesgo en el futuro.

La misión del forense tecnológico es, por tanto, dar respuesta al mayor número de cuestiones que puedan formularse. Evidentemente, estas variaran en función de los objetivos específicos que se persigan con el análisis, pero como premisa inicial algunas de las cuestiones básicas pueden ser las siguientes:

- Fecha y hora exacta en la que se ha producido el ataque o intrusión
- Identificación del atacante
- Técnica o técnicas utilizadas para el ataque o intrusión
- Daños o modificaciones que se han producido mediante el ataque o intrusión

Una vez finalizada la investigación forense, si los resultados, como mínimo, no contestan estas cuestiones, no serán adecuados y no se habrá cumplido el objetivo completamente. Si podemos contestar, pero no de forma correcta, puede que se repitan futuras incidencias, realizadas por el mismo atacante o usando la misma vulnerabilidad Por el contrario, si hemos dado respuesta a las cuestiones planteadas con un adecuado tratamiento de las evidencias, la información obtenida puede ser de muchísima utilidad en nuestras investigaciones presentes y futuras: fraudes, delitos de menores, delitos corporativos, etc.

Para acabar con esta introducción a la investigación y el análisis forense tecnológico, nos gustaría resaltar que debemos cumplir, como en otras técnicas forenses, unos mínimos requisitos que enumeramos a continuación:

- Evitar la contaminación de las pruebas y evidencias digitales
- Actuar metódicamente para que cada paso que demos se pueda verificar a posteriori y que se puedan emplear con otros fines, como, por ejemplo, en un juicio.
- Tener control todo el tiempo de la cadena de custodia de las evidencias digitales; es decir, conocer quiénes han tenido acceso a la evidencia, cuándo, dónde, etc., de forma que se pueda demostrar siempre que la misma no ha sido saboteada o modificada.

2. ESTÁNDARES Y GUÍAS

Todas las normas, guías y estándares que vemos en este punto tienen como finalidad ofrecer una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales. Estos documentos deben dar respuesta a los equipos investigadores forenses para trabajar con las infracciones legales e incidentes informáticos y telemáticos en las distintas empresas y entidades.

1.– Norma UNE 197010:2015: Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)

Esta norma define cómo debe redactarse un informe pericial informático, telemático o tecnológico -o sea, TIC-, sin entrar a valorar ni el aseguramiento de la escena, ni la recolección, ni la preservación, ni el análisis de las evidencias.

Es una actualización de la Norma UNE 197001:2011 “Criterios generales para la elaboración de informes y dictámenes periciales”, que es la norma que especifica los requisitos para la elaboración de los informes y dictámenes periciales. Será el documento base que utilizaremos al pie de la letra para la redacción de los informes en las investigaciones forenses.

2.– Familia UNE 71505:2013

- UNE 71505-1:2013: Tecnologías de la Información (TI). Sistemas de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales.
- UNE 71505-2:2013: Tecnologías de la Información (TI). Sistemas de Gestión de Evidencias Electrónicas (SGEE). Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas.
- UNE 71505-3:2013: Tecnologías de la Información (TI). Sistemas de Gestión de Evidencias Electrónicas (SGEE). Parte 3: Formatos y mecanismos técnicos.

Estas normas UNE nos indican la forma de gestionar evidencias electrónicas y establecen sus buenas prácticas. Ello revertirá en la admisibilidad de las pruebas electrónicas durante los procesos judiciales.

Estas normas nos ayudan a no perder las evidencias o a que las que utilicemos no se puedan poner en duda. En cada una de sus fases de gestión (definición, recogida, custodia y aportación) es fundamental conocer los aspectos jurídicos necesarios para garantizar la eficacia probatoria de las evidencias informática y/o telemáticas, como, por ejemplo, los WhatsApps, las fotos, los mails o la geolocalización.

3.– UNE 71506:2013

Esta norma UNE es el marco de referencia de buenas prácticas en la gestión de evidencias electrónicas, y en ella se fija el procedimiento de análisis forense dentro del proceso de la gestión de las pruebas tecnológicas, basándose en la norma UNE 71505. En la norma hay anexos muy útiles, como un modelo de informe pericial, en el que toma como referencia el modelo de informe ya propuesto en la norma UNE 197001.

También hay un anexo que se refiere al equipamiento para el análisis forense de las evidencias informáticas y telemáticas. Se debe contar con herramientas de *hardware* y de *software* reconocidas por la comunidad internacional forense a pesar de no existir una normalización. Nuestra forma de trabajar en este punto debe, como mínimo, utilizar tres softwares o hardwares para llegar a la misma conclusión. De este modo, somos nosotros mismos los que marcamos el listón alto en cuanto a *software* y *hardware* reconocido y válido.

4.– RFC 3227. Directrices para la recopilación de evidencias y su almacenamiento

Este documento, que se considera un estándar, nos indica las principales guías para la recolección y el almacenamiento de evidencias digitales. El o la forense debe preocuparse en no perder información. En ocasiones deberemos decidir si se deben extraer evidencias de sistemas encendidos

durante una intervención, o si se debe desconectar la máquina de la red para poder evitar que se active cualquier tipo de *malware* que pueda comprometer la información de las unidades conectadas al sistema.

5.– RFC 4810. Como preservar la información a largo plazo

Esta RFC nos define un estándar relacionado con la preservación de la información. Este punto es muy importante para los informes forenses y las investigaciones tecnológicas, ya que nuestro trabajo siempre debe poder ser comprobado para validar su autenticidad y veracidad. Entre otras cuestiones, indica a los forenses TIC cómo debemos proceder para verificar una firma digital tras haber pasado un gran lapso de tiempo desde la generación de esta.

6.– ISO/IEC 27037:2016. Indicaciones para la identificación, recolección, adquisición y preservación de la evidencia digital

Este estándar nos proporciona directrices para la identificación, recolección, adquisición y preservación de potenciales evidencias telemáticas e informáticas que pueden tener valor probatorio. Nos proporciona, entre otras cuestiones, guías para el manejo de evidencias digitales, así como orientaciones en los procedimientos de intercambio de dichas evidencias. Sin embargo, nunca entra en el análisis de la evidencia.

Además, nos indica cómo preservar la evidencia y la cadena de custodia para dispositivos digitales de almacenamiento de todo tipo. Se puede utilizar a la par que la RFC 3227, aunque más bien es una actualización.

7.– ISO/IEC 27040:2105. Almacenamiento seguro

Reúne guías y recomendaciones para que el almacenamiento de las evidencias digitales sea seguro. Nos presenta riesgos existentes en el almacenamiento y nos provee directrices o buenas prácticas incluyendo modelos de auditorías y revisiones para poder controlar el almacenamiento de las evidencias y garantizar que se haga de forma correcta y segura.

8.– ISO/IEC 27042:2015. Indicaciones para el análisis e interpretación de la evidencia digital

Esta norma trata el análisis y la interpretación de evidencias digitales. Proporciona guías sobre cómo un forense puede afrontar el análisis e interpretación de una evidencia digital o tecnológica en un incidente o en una intervención, desde su identificación y análisis, hasta que es aceptada como prueba en un juicio. También señala las partes que deben tener el informe.

Define asimismo conceptos como examen, análisis e interpretación y nos habla de los modelos de análisis que pueden utilizar los investigadores forenses: estáticos, en vivo y en vivo de sistemas, que pueden ser copiados o que se puede obtener una imagen de los mismos.

9.– RFC 4998. Evidence Record Syntax

Esta RFC define un estándar para la preservación de la información, incluyendo información firmada digitalmente. Nos indica cómo demostrar su existencia e integridad durante un periodo de tiempo que se desconoce.

También define el tipo de sistemas de ficheros que pueden ser utilizados en esas situaciones y los requisitos que debe cumplir el registro de evidencias, al que investigadores telemáticos o informáticos pueden hacer referencia para garantizar que dicha información existe y evitar que sea rechazada.

10.– RFC 6283. XML Evidence Record Syntax

Esta RFC nos demuestra la existencia, integridad y validez de la información durante periodos determinados de tiempo. También define la sintaxis en lenguaje XML, así como las reglas de procesado, que deben seguirse para la creación de evidencias íntegras de información, y así evitar que sea rechazada.

3. PRINCIPIOS DEL ANÁLISIS FORENSE TECNOLÓGICO: LA EVIDENCIA DIGITAL

En el día a día de las técnicas forenses tecnológicas, la capacidad de tomar decisiones y dar respuestas rápidas deben equilibrarse con la paciencia. La paciencia es una parte más del trabajo del forense, ya que de ella depende mucho el éxito o el fracaso de su trabajo. La paciencia nos sirve para poder hace frente a dos tareas fundamentales del análisis forense tecnológico:

- Examen en vivo, ON: sucede cuando las pruebas digitales todavía están en funcionamiento, no se han desconectado y el dispositivo para recuperarlos es accesible para ser examinado.

- Examen Post Mortem, OFF: el cibercrimen ya se ha cometido. Las pruebas pueden encontrarse en cualquier sitio, así que el trabajo será mucho más difícil dado que los cibercriminales pueden haber utilizado contramedidas forenses para complicar la investigación. Estudiar e investigar una vez muerto, o *post mortem*, normalmente implica que los dispositivos electrónicos, informáticos o telemáticos que pudieran contener las pruebas se han apagado antes de que llegáramos nosotros a realizar la investigación tecnológica. Es la situación más normal que encontramos los investigadores forenses, de ahí nuestro nombre.

Como ya conocemos, la técnica forense informática tiene como fin aplicar los estándares y procedimientos de la disciplina forense general aplicada a la investigación del análisis de datos, redes y evidencias digitales. Definimos la evidencia digital como cualquier registro generado o almacenado en un sistema digital que pueda ser utilizado como prueba en un proceso. La informática y la telemática forense tienen como base el estudio de todo tipo de evidencia digital involucrada en un incidente con el fin de conseguir convertir esta evidencia en un instrumento de valor legal en procesos judiciales, auditorias, consultorías, investigaciones, etc.

El concepto de evidencia digital viene definido en el artículo 299.2 de la Ley de Enjuiciamiento Civil, donde admite como medio de prueba “los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas”. En su apartado 3 nos habla de “cuando por cualquier otro medio no expresamente previsto (…) pudiera obtenerse certeza sobre hechos relevantes, el Tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias.”

Sin evidencias digitales demostrables e inviolables no tiene razón el 80% del trabajo de investigadores forenses ni de peritos tecnológicos.

Las evidencias digitales son muy difíciles de tratar y de investigar porque poseen características que hacen que el reto sea mayúsculo para el forense tecnológico. Pueden ser volátiles, anónimas, duplicables, alterables, modificables y eliminables. Por lo tanto, dichas pruebas digitales deben cumplir ciertos requisitos para ser aceptadas en un proceso. Estos son:

- Admisible: la prueba debe estar relacionada con el acto que se quiere demostrar.
- Auténtica: la prueba debe ser real y debe estar relacionada con el incidente de forma adecuada.
- Completa: la prueba debe demostrar la actividad al completo.
- Confiable: la prueba debe probar ser auténtica y veraz.
- Creíble: la prueba debe ser clara e inteligible para los jueces.

Diversos ejemplos de evidencias digitales:

- Fecha de último acceso a un fichero o aplicación
- Un registro de acceso en un *router*
- Una *cookie* de navegación web almacenada en un disco duro
- El tiempo que lleva encendido un sistema
- Un fichero en disco
- Un proceso en ejecución en un *switch* gestionable
- Archivos temporales de un teléfono inteligente
- Restos de la instalación de un *software* en un iPhone
- Un disco duro, un *pendrive* u otro dispositivo de almacenamiento.

El estudio de las evidencias encontradas dará información concreta y verificable. Es, por tanto, muy importante que sean recogidas todas las evidencias posibles y que todas sean tratadas de forma responsable, no perturbando el contenido que almacenan y que, evidentemente, cumplan con la cadena de custodia por posibles procesos judiciales posteriores. La labor de forense es importantísima en un proceso judicial.

4. CÓMO TRABAJAR CON LAS EVIDENCIAS DIGITALES EN INVESTIGACIONES FORENSES

En el día a día un investigador o una investigadora forense trabaja con numerosas evidencias digitales, también llamadas registros o evidencias electrónicas. Por ello, se debe establecer, siguiendo las normas, un ciclo de administración que consta de los siguientes pasos:

1.– Evidencias reales y que se puedan corroborar

Debemos tener unos objetivos finales muy claros con el fin de que nuestra prueba sea admitida:

- Establecer la relevancia de los registros electrónicos o evidencias digitales, identificación y comprobación de que están disponibles y se pueden utilizar.
- Comprobar que dichos registros electrónicos tienen un autor que se pueda identificar.
- Comprobar que los registros electrónicos cuentan con una fecha y hora de creación o alteración.
- Comprobar que los registros electrónicos y/o evidencias digitales cuentan con elementos que nos permitan validar su autenticidad.
- Verificar la confiabilidad de la producción o generación de las evidencias digitales por parte del sistema de información.

2.– Estudiar la forma de trabajar con dichas evidencias

En este segundo paso tenemos como objetivos:

- Estudiar el sistema o tecnología de información que produce los registros electrónicos.
- Identificar al autor de los registros electrónicos almacenados.
- Identificar la fecha y hora de creación.
- Verificar que la aplicación se encuentra operando de manera correcta en el momento de la generación de los registros, bien sea en su creación, bien sea en su modificación.
- Verificar la completitud de los registros generados.

3.– Estudiar la forma de recoger sin modificar las evidencias

Aquí tratamos de localizar toda la evidencia digital, asegurando que ninguno de los registros electrónicos originales sea alterado. Para ello consideramos:

- Establecer buenas prácticas y estándares para la recolección de evidencias digitales.
- Preparar evidencias para ser utilizadas en la actualidad y en tiempo futuro.
- Mantenimiento y verificación de la cadena de custodia.
- Verificar el cumplimiento de las regulaciones y normativas alrededor de la recolección de la evidencia digital.

- Desarrollo de criterios para establecer la relevancia o no de la evidencia recolectada.

4.– Estudio y análisis de las evidencias

Una vez que se han finalizado todos los pasos anteriores, estando en disposición de la búsqueda de los datos requeridos y su debida cadena de custodia, es el momento de comenzar con el análisis de las evidencias digitales para establecer los hechos ocurridos en el contexto de la situación bajo análisis o establecer si hace falta buscar más evidencias para completar o aclarar los hechos bajo estudio o investigación.

5.– Presentación de los resultados

Tras ello, realizaremos un reporte preciso y completo presentando los resultados del análisis y los hallazgos encontrados. La documentación debe ser completa, precisa, comprensiva y auditable. Aconsejamos:

- Documentar los procedimientos efectuados por el profesional a cargo.
- Mantener una bitácora de uso y aplicación de los procedimientos técnicos utilizados.
- Cumplir con exhaustivo cuidado con los procedimientos previstos para el mantenimiento de la cadena de custodia. Este paso es importantísimo e imprescindible en la labor forense.

6.– Valoración de las evidencias

Vamos ahora a determinar la relevancia del resultado del estudio de las evidencias digitales, identificando aquellas evidencias que demuestren de forma clara y eficaz los elementos que se desean aportar en el proceso y/o en un juicio que se lleve a cabo. En síntesis, se trata de realizar una valoración de las pruebas aportadas y jerarquizar aquellas con mayor relevancia.

Para ello, sugerimos varios criterios a tener en cuenta:

- Reglas de la evidencia, que indican que se han seguido los procedimientos, y reglas establecidas para la adecuada recolección y manejo de la evidencia.
- Valor probatorio, que nos indica aquella evidencia digital que tenga signo distintivo de autoría, autenticidad y que sea fruto de la correcta operación.

7.– Estudiar la posible admisibilidad de las evidencias digitales

Dada la fragilidad y la volatilidad de la evidencia digital, es especialmente importante marcar énfasis, dentro del proceso de análisis de la evidencia digital, en el uso de una estrategia de formalización que ofrezca admisibilidad de la misma.

En general, las instituciones de justicia basan esta admisibilidad apoyándose en estos cuatro conceptos:

- **Autenticidad**: busca confirmar que las evidencias aportadas corresponden a la realidad de la escena del crimen y que los medios originales no han sido alterados.

- **Confiabilidad**: demuestra si los elementos probatorios aportados vienen de fuentes creíbles y verificables.

- **Suficiencia**: este aspecto se refiere a que la evidencia presentada debe ser suficiente como para poder adelantar el caso.

- **Conformidad con las leyes y reglas de la administración de justicia**: hace referencia a los procedimientos internacionalmente aceptados para recolección, aseguramiento, análisis y reporte de la evidencia digital.

5. EVIDENCIAS DIGITALES EN CASOS REALES

El tema de las evidencias digitales ya ha sido tratado por el TS en su sentencia de la Sala Segunda de 19 de mayo de 2015, donde se enjuiciaba la validez y autenticidad de unos pantallazos extraídos de una red social en un caso de acoso sexual. En ella establecía que la carga de la prueba de la idoneidad probatoria de las capturas de pantalla o archivos de impresión corresponde a quien pretende aprovechar dicha prueba, por lo que, a falta de su reconocimiento por la otra parte, será necesario un informe pericial -que incluya la investigación forense en su interior- que identifique el emisor de los mensajes delictivos o una prueba testifical que acredite su remisión.

La sentencia del párrafo anterior ya ha sido reiterada en otra sentencia, de 27 de noviembre de 2015, de la Sala Segunda del TS, que señala la posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, aparte del anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, lo que hace perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. En este sentido, resulta indispensable que un perito telemático identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido.

El TSJ de Galicia, en la Sala de lo Social, en su sentencia de 28 de enero de 2016 distingue cuatro supuestos para aceptar un documento o mensaje de los llamados de mensajería instantánea:

- Cuando la parte interlocutora de la conversación no impugna la conversación.

- Cuando reconoce expresamente dicha conversación y su contenido.

- Cuando se compruebe su realidad mediante el cotejo con el otro terminal implicado (exhibición).

- Cuando se practique una prueba pericial que acredite la autenticidad y envío de la conversación para un supuesto diferente de los anteriores.

En definitiva, debemos tratar de llevar al proceso en el que estemos inmersos todo tipo de evidencias que permitan trasladar al órgano judicial la necesaria convicción sobre la autenticidad de la evidencia digital aportada, de modo que podamos acreditar la autenticidad de la misma y protegernos ante la hipotética impugnación de la contraparte. Evidentemente, para ello entra en juego la investigación y el análisis forense tecnológico.

6. EJEMPLOS DE INVESTIGACIÓN Y ANÁLISIS FORENSE TELEMÁTICO

Aunque los análisis forenses telemáticos pueden resultar bastante difíciles por todos los conocimientos técnicos que se requieren, vamos a ver algunas nociones básicas en la actividad diaria.

FIREWALL

El *firewall*, que puede ser un dispositivo *software* o *hardware*, nos permite controlar las conexiones entre dos *hosts* de una red. Los *firewalls* siempre tienen registros para consultar los detalles de sus acciones y de su funcionamiento. Gracias a estos registros podemos encontrar patrones de ataque e intentos de entrar en nuestro *firewall* o en nuestra red.

Los registros, para un investigador o una investigadora forense tecnológico, deben ser una prueba irrefutable, ya que la integridad de estos es fundamental. Cada archivo o *log* está marcado con una fecha y hora. Estos registros son importantísimos, ya que no solo registran cada paquete de la red, sino que lo hacen para cada petición y para cada conexión. Es una herramienta fundamental para el administrador de una red, así como para el investigador forense, pues al final lo que se busca son las conexiones entre dos direcciones IP en concreto, o el envío de ficheros entre dos conexiones.

SNIFFERS O 'ESNIFADORES DE RED'

Los *sniffers* tiene la responsabilidad de realizar la captura de distintos paquetes que se encuentren en circulación a través de una red de datos. Estos no se limitan a capturar paquetes sin más, sino que disponen de la inteligencia para analizar la topología de la red y de llevar a cabo capturas direccionadas.

Los *sniffers* se utilizan para analizar los paquetes de red y estudiarlos, no solo de capturarlos. Debido a ellos, para los investigadores forenses telemáticos es una herramienta fundamental y muy utilizada. En el siguiente punto de herramientas veremos alguno gratuito y muy potente.

Este *software* analiza los paquetes y los datos que se envían. De estos datos se obtienen análisis e informes, como puede ser el caso del remitente de la información, del destinatario de la misma, el servidor que se ocupa del proceso o el tipo de paquete que se está transmitiendo. Estos datos son valiosísimos, dado que con el *sniffer* adecuado podemos proporcionar información muy precisa que podría llegar incluso a transcribir una conversación por mail.

Los *sniffers* pueden ser activos (que buscan) o pasivos (que escuchan), pero ambos te devolverán los paquetes que cumplan con tu criterio de búsqueda. Lo que le interesa a un investigador forense es capturar, almacenar y transmitir esos paquetes de tu red sin añadir datos innecesarios a la red.

Existe una gran variedad de herramientas de código abierto que deberían formar parte del kit de cualquier recopilador de pruebas, empezando por el famosísimo Wireshark. Dado que el tráfico de red consiste en paquetes de datos o fragmentos de información, Wireshark los capturará y anali-

zará. En lugar de tener que buscar línea por línea en cada paquete para identificar en las cabeceras la información de enrutamiento, el remitente y el contenido de cada paquete, Wireshark se encargará de hacer el trabajo pesado por ti. Además, es una herramienta multiplataforma.

*ROUTER*S Y *SWITCH*ES GESTIONABLES

Como hemos visto en los registros de los *firewalls*, los registros de los *router*s y *switch*es gestionables (estos son capa 3) recopilan detalladamente las actividades típicas de estos equipos. En ocasiones aparecerá en ellos algún dato que atraerá el interés del investigador forense.

Aparte del hecho de ser una prueba de que sucedieron ciertos eventos, los registros resultan difíciles de manipular. Las herramientas de *software* tienen programas que automatizan el filtrado de registros.

CABECERAS DE LOS EMAILS

Los emails contienen información sobre cada equipo por el que pasan hasta que llegan al destino. Esta se añade a la cabecera que contiene la información del correo. Seguramente, la información más importante y relevante desde el punto de vista forense se encuentra en las cabeceras. No obstante, ver las cabeceras no resulta siempre sencillo.

Para leer las cabeceras debemos hacerlo al revés. ¿Por qué? En lo más alto de la lista está el receptor, y por cada ruta que atraviesa el correo se añade una línea hasta llegar a la última que es donde se refleja desde qué red o equipo se envió el correo.

Esto sólo valdrá si el emisor del correo utilizó su dirección de correo real para enviarlo. Los correos se pueden falsificar, las IP se pueden alterar y hay toda clase de trucos que se pueden emplear para ocultar el emisor real. Las cabeceras pueden proporcionarte pistas, pero no esperes resolver ningún caso basándote únicamente en la información de las cabeceras del correo, aunque puedes acercarte a ello.

7. HERRAMIENTAS FORENSES

Una de las preguntas más extendidas siempre es: ¿cuáles son las mejores herramientas para trabajar como forense tecnológico? La respuesta, como podréis comprender, es casi imposible de contestar porque existen programas, aplicaciones y herramientas que no cesan de evolucionar, y de lo que hablemos en este ebook, en 5 meses habrán aparecido herramientas mejores y más actualizadas.

Aun así, vamos a estudiar algunas de ellas, la mayoría gratuitas, que nos ayudarán en el campo del análisis forense en informática y telemática para resolver casos simples como análisis de memoria, de discos duros, de imágenes o de captura de todo lo que pase por una red, entre otras cosas.

1.– Grabación de acciones (*Problem Steps Recorder*)

En Windows 7, 8 y 10 se puede localizar una pequeña utilidad muy práctica llamada *Problem Steps Recorder (psr.exe)*. La grabación de acciones registrará las interacciones paso a paso que se producen cuando el usuario reproduce el problema; pemite realizar capturas de pantalla de cada acción. Luego, puedes utilizar esta información en un informe con datos detallados y los registros de errores relevantes. Esta herramienta es ideal para estudiar los problemas de un usuario, o para que un notario, después de dar fe, pueda llevarse pruebas con la consiguiente cadena de custodia.

Para iniciar el *Problem Steps Recorder*, vaya a ejecutar y escriba *psr.exe*. Haga clic en 'Iniciar Grabación' y la herramienta registra cada interacción a partir de ese momento. Se pueden agregar comentarios durante el proceso.

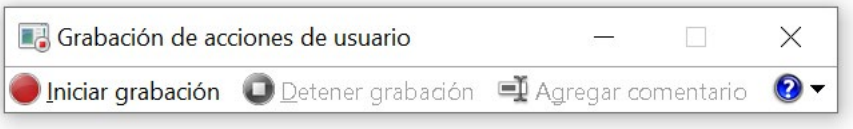


Imagen 1. Captura de pantalla de Problem Steps Recorder. Fuente: Elaboración propia.

2.– WELT (Windows Error Lookup Tool).

Windows muchas veces nos arroja un error que no sabemos muy bien lo que significa. Esta herramienta nos indica qué significa el código de error y con que está relacionado. Parece una herramienta no muy útil si pensamos que escribiendo el error en Google seguramente obtendremos información, pero muchas veces no podemos tener conexión a internet en alguna investigación por temas de cadena de custodia, por lo que se convierte en una herramienta bastante útil.

3.– WinAudit

Como parte del proceso de solución de problemas, es útil saber la mayor información posible sobre la máquina donde reside el problema para ayudar a encontrar una solución más rápidamente. WinAudit analiza el equipo y reúne toda una serie de información sobre el *software* instalado, TCP/IP, unidades, registros, etc.

Para iniciar una auditoría de su equipo local, sólo tiene que ejecutar WinAudit para iniciar la aplicación. Una vez que se haya completado, se puede comenzar a revisar la información de las diferentes categorías en el panel de la izquierda, o guardar la información en un archivo PDF/CSV/TXT/HTML.

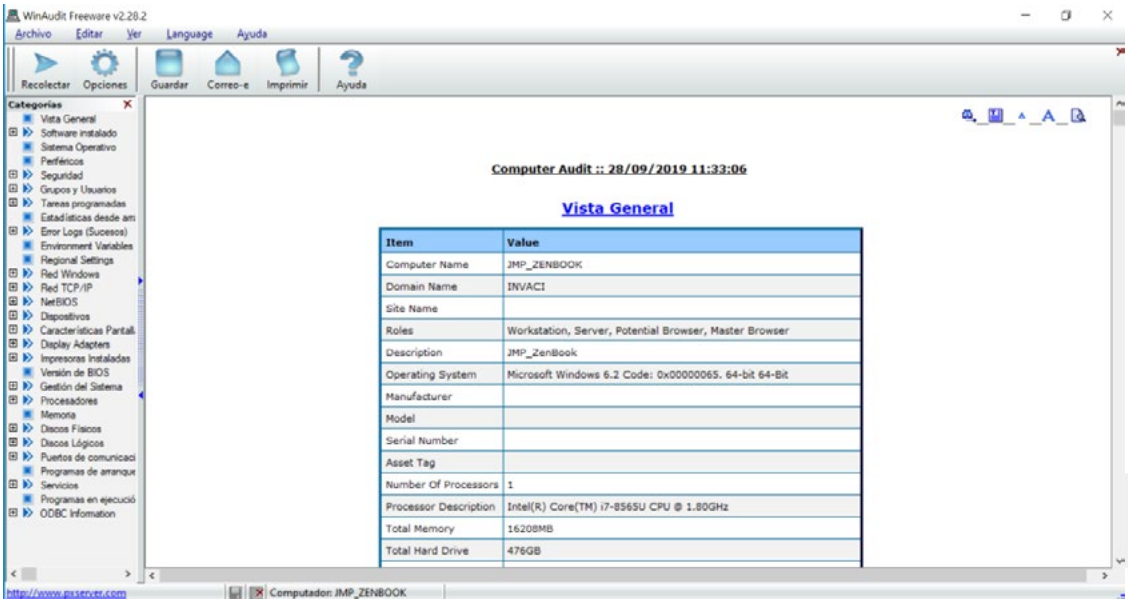


Imagen 2. Captura de pantalla de WinAudit. Fuente: Elaboración propia.

4.– NirLauncher Nirsoft

NirLauncher es una aplicación que agrupa a más de 170 utilidades gratuitas portátiles. Las herramientas disponibles incluyen herramientas de recuperación de la contraseña, herramientas de internet, herramientas de programación y herramientas del sistema. Todas ellas pueden ser utilizadas para la recopilación de información y la resolución de problemas.

Entre las más importantes para el análisis forense, está **USBDeview**, que nos muestra todos los dispositivos USB actuales y conectados anteriormente en un equipo local o remoto al tiempo que nos aporta numerosa información de cada uno de ellos. También es útil**CurrPorts**, que nos muestra una lista de todos los puertos TCP/UDP abiertos actualmente en la máquina local y nos ofrece información sobre el proceso que abrió el puerto, en qué momento lo creóy el usuario que lo creó. También puede cerrar conexiones abiertas y exportar la información a un archivo.

Imagen 3. Captura de pantalla de NirLauncher Nirsoft. Fuente: Elaboración propia.

5.– WSCC (*Windows System Control center*)

WSCC no es una herramienta de solución de problemas en sí, pero la facilita. Permite instalar, actualizar, ejecutar y clasificar toda la colección de herramientas en un solo lugar, de entre más de 270 herramientas.

6.– Xirrus WIFI Inspector.

WIFI Inspector es un potente gestor de WIFI y una herramienta de solución de problemas que permite localizar y verificar los dispositivos WIFI, detectar puntos de acceso, solucionar problemas de conexiones y la búsqueda de redes WIFI.

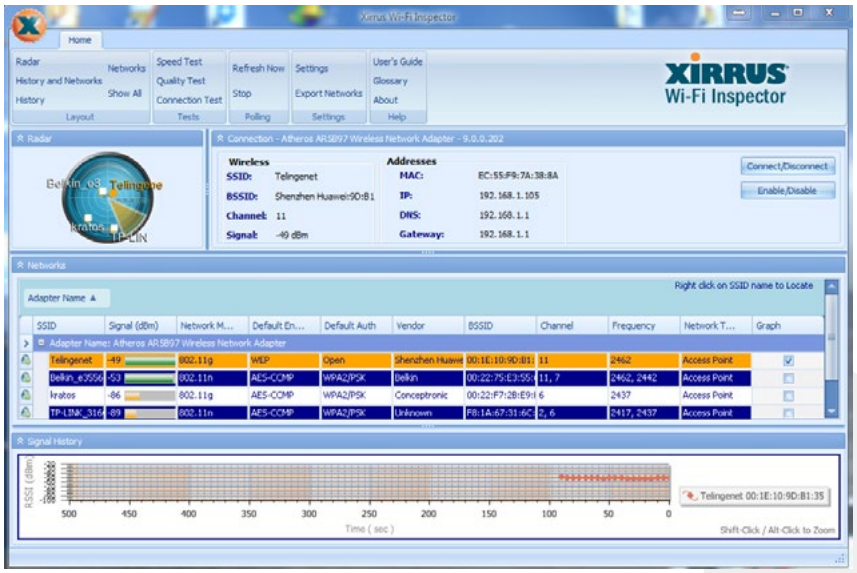


Imagen 4. Captura de pantalla de Xirrus WIFI Inspector. Fuente: Elaboración propia.

7.– Whois

Whois realiza una búsqueda de la información de registro de una determinada dirección IP o nombre de dominio.

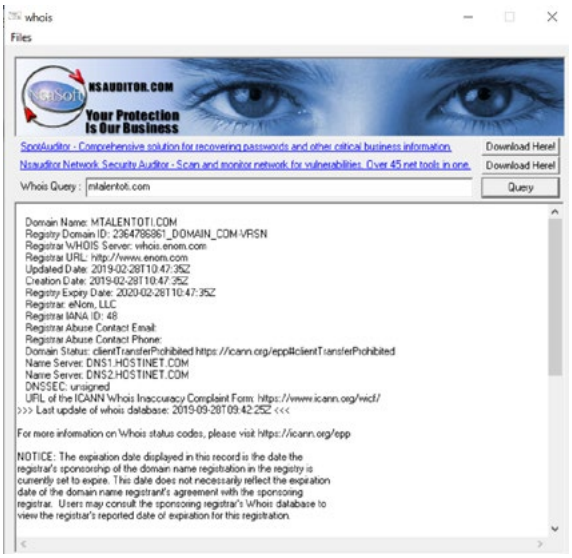


Imagen 5. Captura de pantalla de Whois. Fuente: Elaboración propia.

8.– ShareEnum

Un aspecto de la seguridad de red de Windows que se suele pasar por alto son los recursos compartidos de archivo. Se produce una brecha de seguridad común cuando los usuarios definen los recursos compartidos del archivo con bajos niveles de seguridad, lo que permite que los usuarios no autorizados vean archivos privados. No existen herramientas integradas para listar los recursos compartidos visibles en una red ni su configuración de seguridad, pero ShareEnum llena este vacío y permite bloquear los recursos compartidos de archivo de la red.

Cuando se ejecuta ShareEnum, usa la enumeración NetBIOS para analizar todos los equipos dentro de los dominios accesibles, y muestra los recursos compartidos de archivo e impresión y su configuración de seguridad. Dado que sólo el administrador del dominio puede obtener acceso a todos los recursos de red, ShareEnum es más efectivo si se ejecuta desde una cuenta de administrador de dominio.

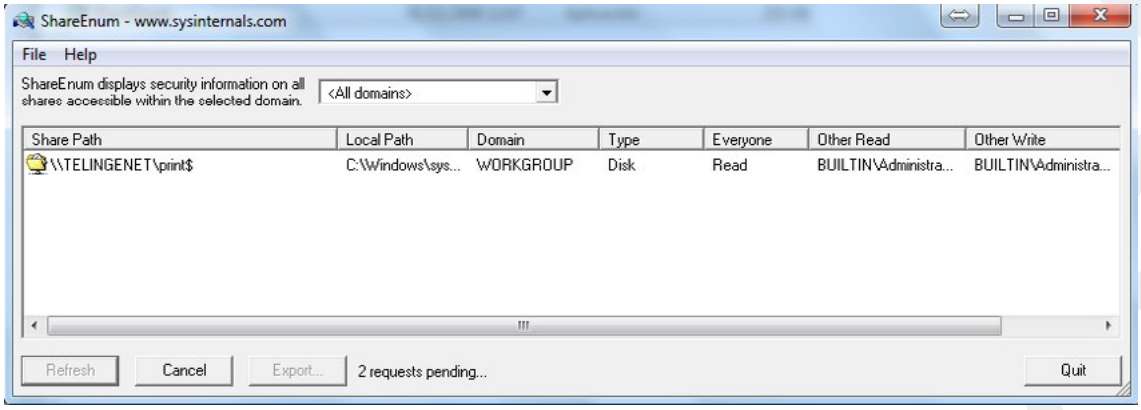


Imagen 6. Captura de pantalla de ShareEnum. Fuente: Elaboración propia.

9.– TCP View

TCPView es un programa de Windows que muestra listados detallados de todos los extremos de TCP y UDP del sistema, incluidas las direcciones locales y remotas y el estado de las conexiones TCP. En Windows TCPView informa también del nombre del proceso que posee el extremo. Ofrece un subconjunto más informativo y perfectamente presentado del programa Netstat incluido con Windows. La descarga de TCPView incluye TCPVcon, una versión de línea de comandos con la misma funcionalidad.

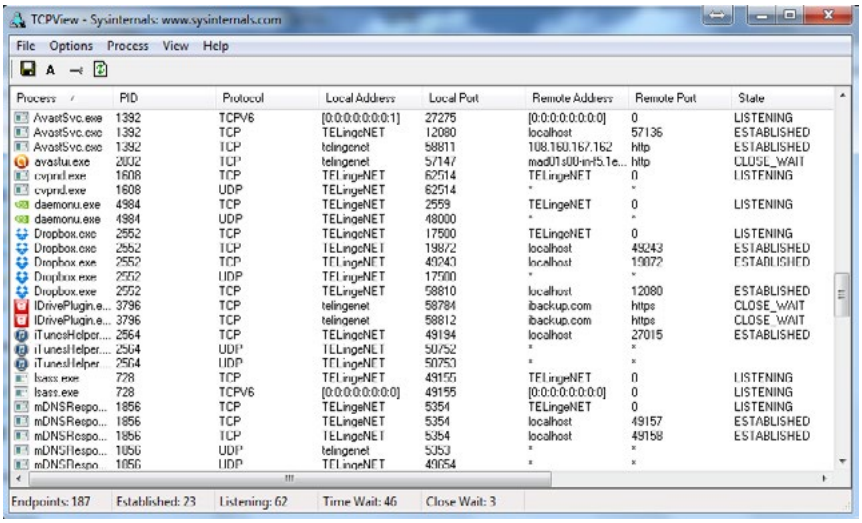


Imagen 7. Captura de pantalla de TCP View. Fuente: Elaboración propia.

10.– The Dude de MicroTik

Este *software* es muy interesante. Puede rastrear automáticamente todos los dispositivos dentro de una subred determinada y luego dibujar y diseñar un mapa de una red, pudiendo después ejecutar diversas acciones sobre cada elemento, ping, tracert, etc.

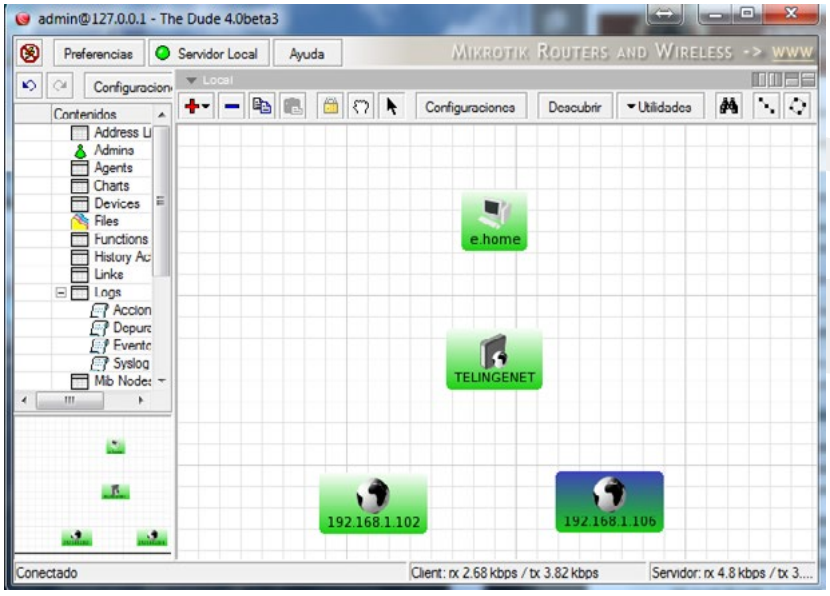


Imagen 8. Captura de pantalla de The Dude. Fuente: Elaboración propia.

11.– Microsoft Baseline Security Analyzer 2.2

Microsoft Baseline Security Analyzer (MBSA) es una herramienta fácil de usar que ayuda a las pequeñas y medianas empresas a determinar su estado de seguridad de acuerdo con las recomendaciones de seguridad de Microsoft y ofrece orientación precisa sobre soluciones. Mejora el proceso de administración de seguridad mediante MBSA para detectar errores de configuración de seguridad habituales e identificar las actualizaciones que faltan en sus sistemas informáticos.

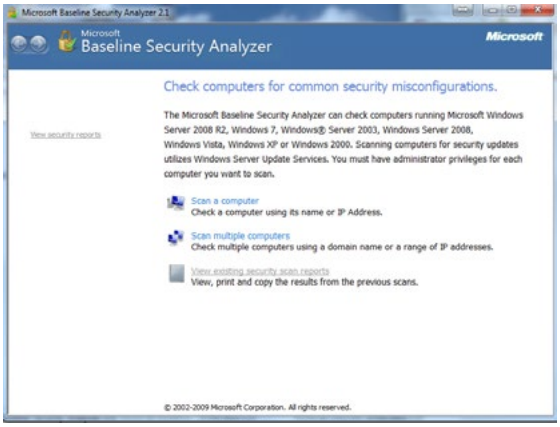


Imagen 9. Captura de pantalla de Microsoft Baseline Security Analyzer. Fuente: Elaboración propia.

12.– Wireshark

Wireshark es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de *software* y protocolos, y como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos.

Permite examinar datos de una red en tiempo real o de un archivo de captura salvado en disco. Se puede analizar la información capturada a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

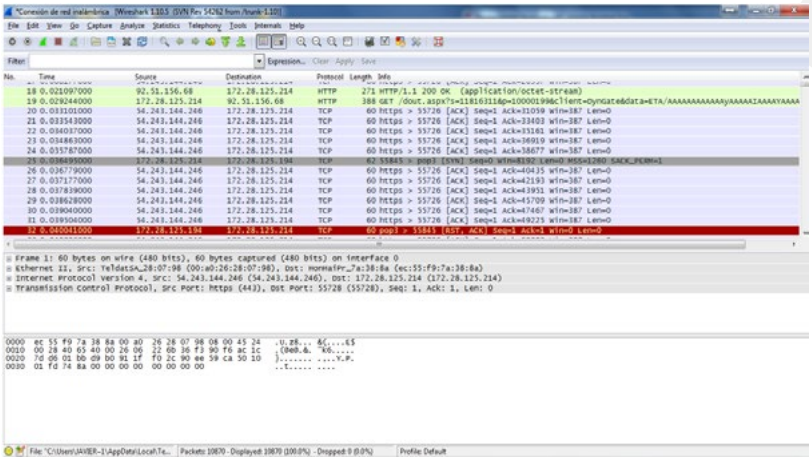


Imagen 10. Captura de pantalla de Wireshark. Fuente: Elaboración propia.

13.– Look @LAN

Permite escanear rápidamente su red en busca de nodos activos. Proporciona monitoreo, reporte, registro y funciones de detección de sistema operativo y sus vulnerabilidades.

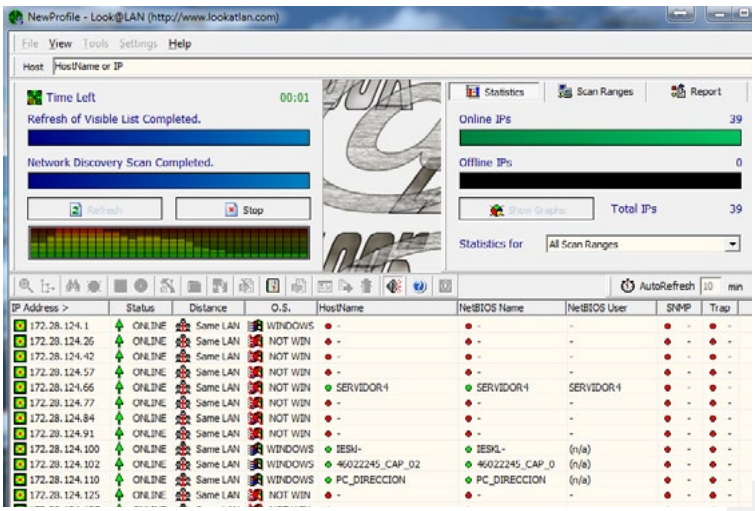


Imagen 11. Captura de pantalla de Look @LAN. Fuente: Elaboración propia.

14.– Capsa Network Analyzer

Permite monitorizar, diagnosticar y solucionar problemas en la red. Es muy potente, pero es gratuita solo unos días. Tras ellos se convierte en *software* de pago.

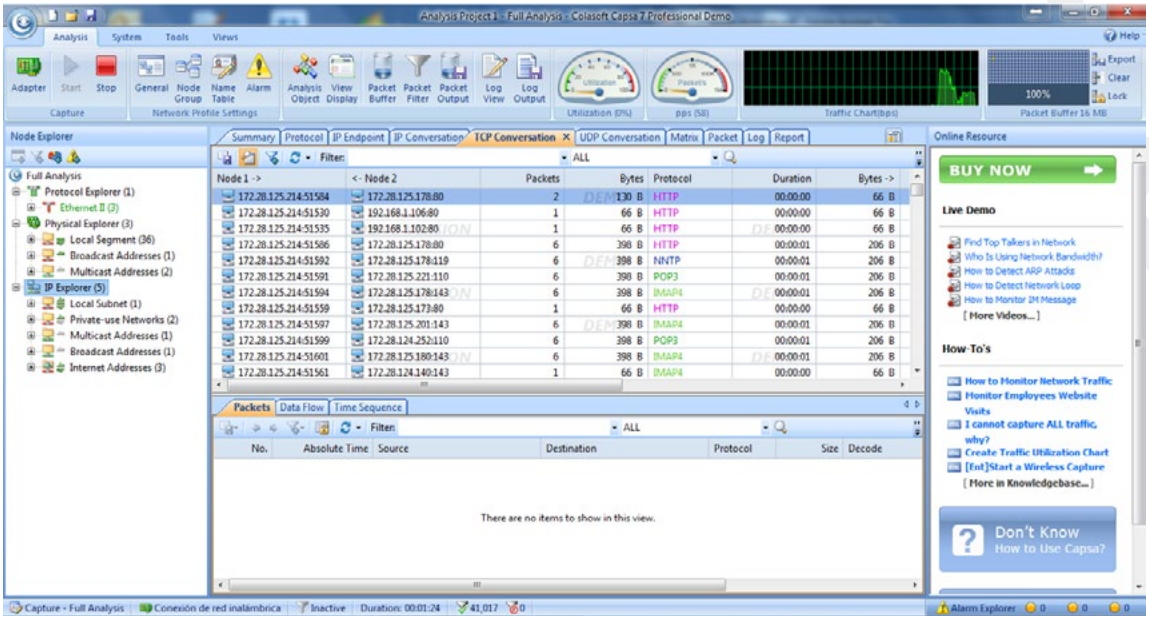


Imagen 12. Captura de pantalla de Capsa Network Analyzer. Fuente: Elaboración propia.

15.– Advanced IP Scanner

Esta herramienta permite realizar un seguimiento y administrar las direcciones IP de la red de forma rápida y sencilla.

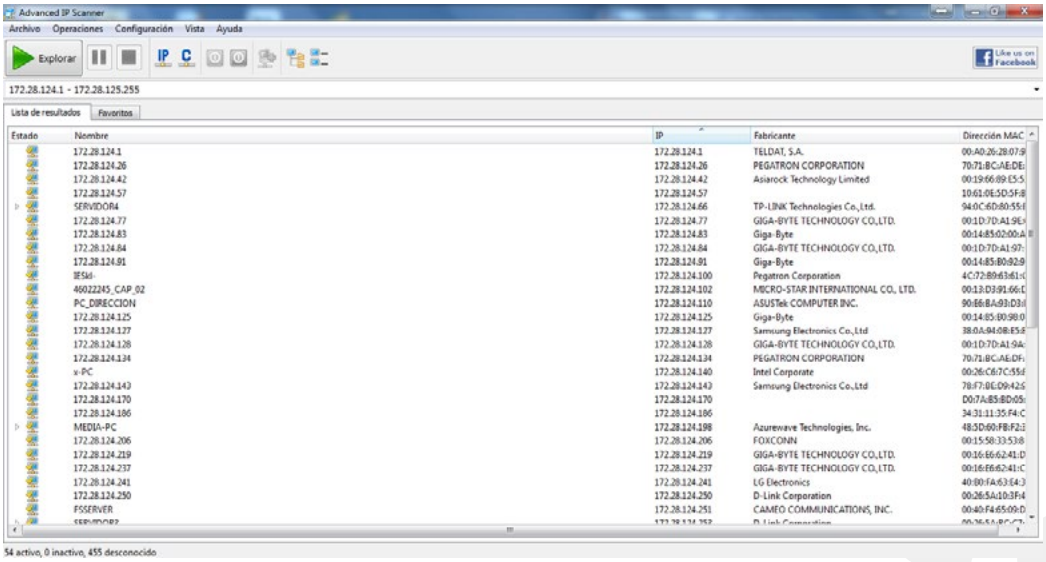


Imagen 13. Captura de pantalla de Advanced IP Scanner. Fuente: Elaboración propia.

16.– PingPlotter

Es una aplicación *tracert* ligera que genera gráficos para ayudar a visualizar la ruta de los paquetes desde el origen al destino.

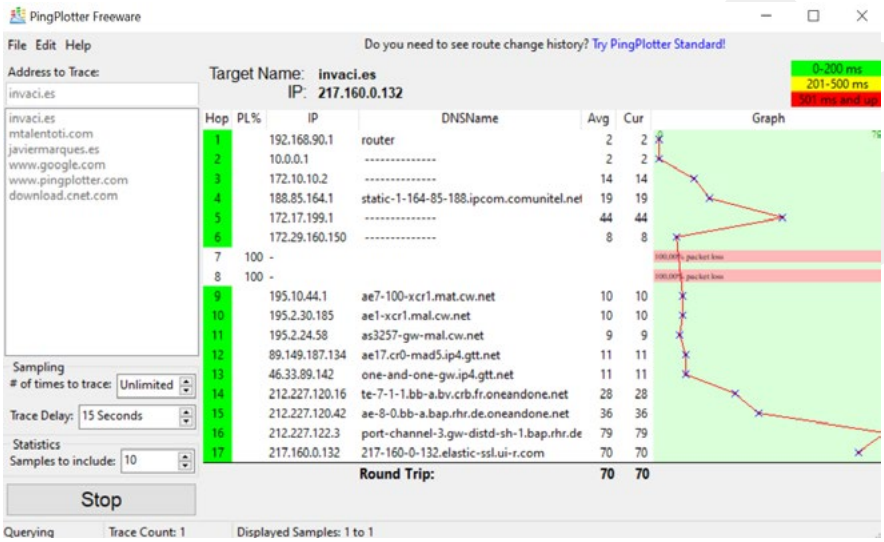


Imagen 14. Captura de pantalla de PingPlotter. Fuente: Elaboración propia.

17.– SolarWinds

Con esta herramienta se puede visualizar rápidamente los permisos de usuario y grupo de una carpeta o unidad compartida en un formato jerárquico. Puede seguir permisos de nivel de acción, ofrecer un desglose del nivel de recurso compartido y permisos a nivel de archivo y ayudar a identificar porqué algunos usuarios tienen los permisos que tienen.

18.– WirelessNetView

Supervisa la actividad de las redes inalámbricas en la zona y muestra información relacionada con ellos, tales como SSID, calidad de señal, MAC, canal, etc.

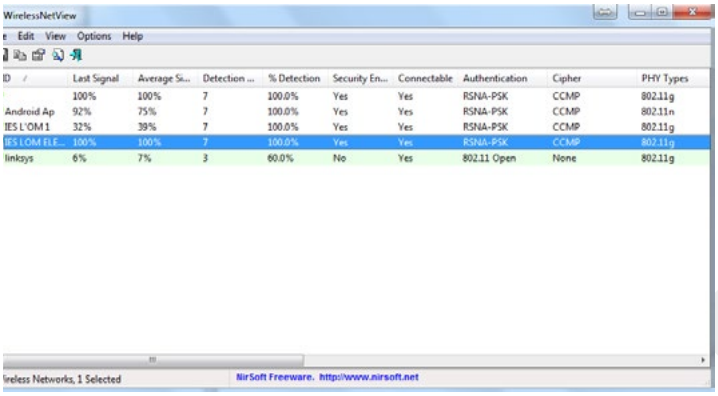


Imagen 15. Captura de pantalla de WirelessNetView Fuente: Elaboración propia.

19.– BluetoothView

Supervisa la actividad de los dispositivos *Bluetooth* en la zona y muestra la información relacionada con ellos, como el nombre del dispositivo, la dirección *Bluetooth* o el tipo de dispositivo, entre otras cuestiones.

20.– Total Network Inventory

Es una aplicación de monitoreo de red integral que le permite ver el estado de su red. Es personalizable y tiene características de alerta, lo que le permite observar cuándo alguna cosa no funciona bien o está mal.

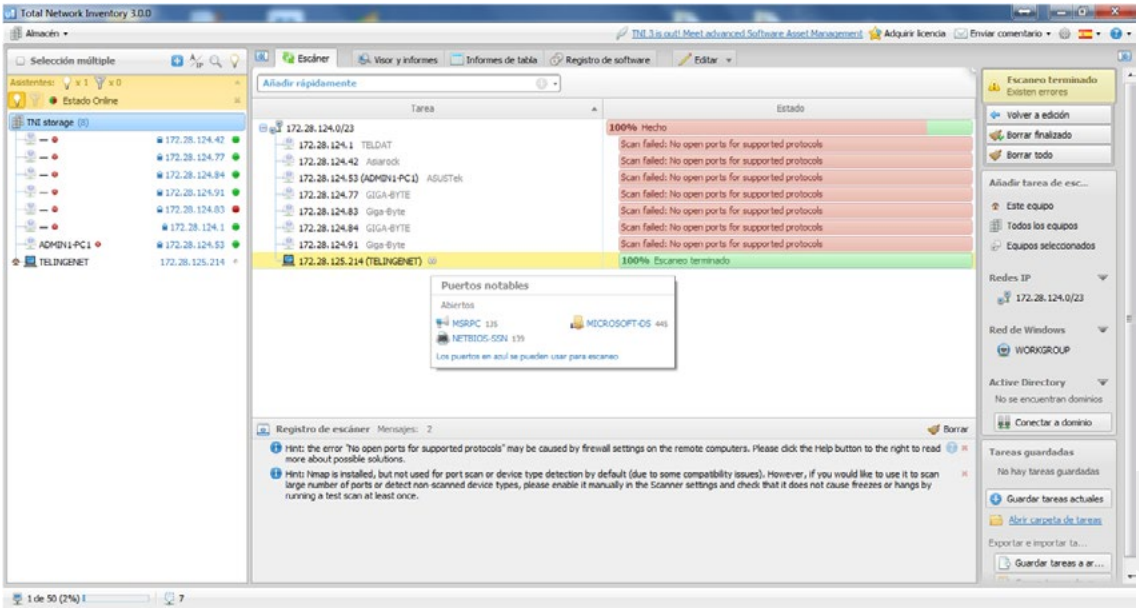


Imagen 16. Captura de pantalla de Total Network Inventory. Fuente: Elaboración propia.

PRUEBAS DEL SISTEMA Y SOLUCIÓN DE PROBLEMAS

21.– Oracle VirtualBox

Es una solución de virtualización gratuita, multiplataforma de uso general que se puede utilizar para crear y ejecutar múltiples máquinas virtuales. Es ideal para entornos de prueba o desarrollo.

22.– RAMMap

Permite analizar la asignación de memoria física en el sistema. Por ejemplo, es capaz de determinar la cantidad de datos de archivo almacenados en la memoria RAM o la cantidad de RAM que es utilizada por los controladores del dispositivo.

23.– AppCrashView

Permite ver el informe de errores de Windows (.wer) de archivos en una interfaz de usuario sencilla y luego guardar los resultados en formato de archivo TXT / CVS / HTML / XML

24.– RootkitRevealer

Le permite detectar la presencia de *rootkits* que funcionan al intentar ocultar sus archivos o entradas del registro.

25.– ManagePC

Le permite crear un inventario de todas sus máquinas en el dominio, incluyendo *hardware*, *software*, dispositivos, parches y políticas de grupo.

26.– Pandora FMS

Es una solución de monitoreo de red que le permite controlar múltiples plataformas, desde máquinas Linux, a la máquina Solaris y las máquinas Windows. Proporciona alertas e informes de CPU, disco y uso de memoria, de la temperatura, o incluso de los valores de la aplicación. Hoy es de pago, aunque hay una demo.

27.– OCS Inventory

Es un inventario automatizado de la implementación de aplicaciones. Esto le permite determinar qué dispositivos o *software* están instalados en su red e implementar *software* o la configuración de secuencias de comandos con una interfaz basada en la Web.

28.– ExtraSpy Employee Monitor

Le permite monitorizar las actividades de los empleados a través de la red para ayudar a detectar el uso indebido de los bienes de la empresa o de las personas improductivas.

29.– AdRestore

Permite recuperar objetos de servidor eliminados de Windows Server Active Directory.

ARCHIVO Y GESTIÓN DE DISCOS

30.– Disk2vhd

Esta herramienta es capaz de sacar una copia online del disco físico sobre el cual está corriendo un sistema operativo posterior a Windows XP SP2 o Windows Server 2003 SP1 y la convierte al formato VHD que usan Windows Virtual PC, Virtual Server e Hyper-V. Y si lo hace sobre el disco de sistema, obviamente también sobre cualquier otro disco/partición de datos presente en el equipo.

31.– Recuva

Con Recuva se puede recuperar archivos que se hayan eliminado accidentalmente de su máquina.

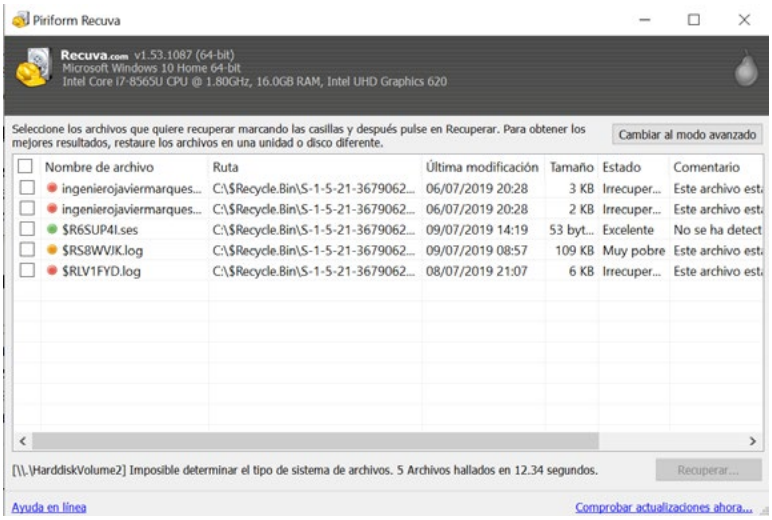


Imagen 17. Captura de pantalla de la plataforma Recuva. Fuente: Elaboración propia.

32.– Bacula

Es un conjunto de aplicaciones que permiten la copia de seguridad, recuperación y verificación de los datos a través de una red.

RENDIMIENTO Y SUPERVISIÓN DE DISPONIBILIDAD

33.– Axence Free Net Tools

Consiste en un conjunto completo de herramientas de seguimiento, análisis de red, seguridad y administración, todo en una interfaz de usuario intuitiva y fácil.

34.– Free IP Tools

Es un conjunto de herramientas comunes que se utilizan para solucionar problemas de las aplicaciones y servicios de red en una única interfaz. Incluye herramientas como PortScan, traceroute y SNMPAudit.

HERRAMIENTAS FORENSES PARA UNA PERICIAL TECNOLÓGICA COMPLETA

35.– Encase

Se trata de una herramienta comercial específica para el análisis forense de sistemas tecnológicos. Entre otras muchas posibilidades, EnCase permite escanear discos, crear imágenes de discos para su posterior análisis, recuperar archivos de unidades que hayan sido formateadas, realizar borrado seguro de unidades a bajo nivel, consultar archivos por tiempos de creación, último acceso y última escritura e identificar extensiones de archivos y múltiples soportes de archivos. Permite el análisis sobre discos duros, dispositivos USB, tabletas y teléfonos inteligentes. Y no solo genera los informes adecuados, sino que además exporta evidencias.

36.– Forensic Toolkit (FTK)

FTK es otro paquete de herramientas forenses muy utilizado por los investigadores forenses informáticos y telemáticos. Al igual que el anterior, se trata de una distribución comercial. Permite el análisis de correo electrónico y de archivos comprimidos, opciones de búsqueda de archivos y restauración de datos, así como múltiples archivos y formatos de adquisición.

37.– Caine *(Computer Aided Investigative Environment)*

Caine es una distribución basada en Ubuntu. Ofrece un completo entorno forense, de modo que integra herramientas de *software* existentes, proporcionando una interfaz gráfica amigable. Precisamente éste es el punto clave de CAINE, su interfaz, que permite una integración sencilla y bastante amigable.

Entre otras posibilidades, permite clonar y montar unidades, manipular volúmenes de diferentes sistemas operativos (Windows 7, 8 y 10, Unix, Macintosh), recuperar archivos o borrarlos de forma segura, recuperar unidades de disco, auditar los dispositivos conectados a la red (incluso determinando qué puertos tienen abiertos), editores hexadecimales, recuperar archivos de imágenes y de

vídeo, recuperar contraseñas, examinar el contenido de los archivos de respaldo que los móviles iPhone dejan en el disco y recuperar datos de DVDs. Además, incluye otras herramientas como Autopsy.

38.– DEFT *(Digital Evidence & Forensic Toolkit)*

DEFT es una distribución basada en Linux. Se trata de un proyecto italiano de gran éxito y que incluye las mejores herramientas forenses. Además de un número considerable de aplicaciones de Linux y scripts, DEFT también cuenta con la suite de DART que contiene aplicaciones de Windows.

39.– SIFT *(SANS Investigate Forensic Toolkit)*

SIFT constituye otra distribución basada en Ubuntu e incluye herramientas como SleuthKit/Autopsy, Wireshark y Pasco.

HERRAMIENTAS *SOFTWARE* PARA TELÉFONOS INTELIGENTES

Los fabricantes de *software* forense han sacado versiones de análisis forense para *smartphones*. Pocas herramientas hay de este tipo que sean gratuitas. Hablamos aquí de unas pocas:

40.– Oxygen

Dispone de varios productos para móviles. Es gratis durante un pequeño periodo de tiempo, y después debemos abonar el pago. Se puede descargar la versión gratuita de Oxygen Forensic Suite (Standard) en https://www.oxygen-forensic.com/es/. Con este *software* podemos, entre otros, leer *backups* de un iPhone.

41.– Bit Pim

Software de código abierto que no funciona con todos los teléfonos inteligentes. Progresivamente van publicándose nuevas versiones de *software*. Lee la documentación de cómo funciona en http://www.bitpim.org

42.– Sleuth Kit

Es otro *software* de código abierto que incluye el análisis forense para terminales móviles. Es muy bueno, y puedes conseguir con él información suministrada en otros muchos productos de pago. Puedes encontrar una *wiki* completa en www.sleuthkit.org

8. CONCLUSIONES

En este capítulo hemos intentado explicar de forma breve, pero con posibilidad de empezar un estudio exhaustivo, términos y conceptos como pruebas forenses, evidencias digitales, investigaciones TIC, pruebas digitales de uso judicial y cadena de custodia. Viendo esta nomenclatura se puede llegar a pensar que el investigador forense tecnológico es un superhéroe de ficción, que trabaja con la Policía Nacional o con el FBI, persiguiendo ciberterroristas o salvando pymes de ataques cibernéticos. Pero la realidad no es esa.

Somos técnicos o ingenieros que nos hemos especializado en este campo que aún está naciendo, y que se encuentra en su germen inicial. Nuestras labores más habituales se centran en disciplinas mucho más cercanas a la realidad del día a día, como pueden ser la recuperación de datos de un disco duro, la extracción de información de una red, la determinación del porqué del borrado de un *log*, el seguimiento de origen y destino de un correo electrónico, la comprobación de una dirección IP o la detección de actividades no contempladas en la política de seguridad TIC de una empresa por parte de un empleado.

En España todavía no hay demanda frecuente de este tipo de trabajos, pero los ingentes casos de fallos de ciberseguridad que cada día aparecen en la prensa o en la televisión están incrementado el interés de las empresas y organismos por estos servicios.

Como profesionales, lo que es necesario es una mayor especialización y reciclaje con el fin de que los resultados sean óptimos. El objetivo es asegurar una excelente gestión por parte de los forenses tecnológicos en el tratamiento de las evidencias digitales, de modo que se garantice su consideración en un juicio o investigación.

Parar, pensar y actuar es nuestro lema. El análisis forense digital necesita formación constante de sus profesionales, ya que evoluciona con rapidez, en muchas ocasiones mucho más de lo deseado. Si no hacemos este reciclaje y formación especializada constante, no será posible que mantengamos el nivel técnico y profesional adecuado como especialistas de esta apasionante profesión, que es la investigación y el análisis forense tecnológico.

CAPÍTULO V

CIBERSEGURIDAD DEL NEGOCIO Y CIBERSEGURIDAD DE LA COMPETENCIA PARA LAS PYMES

V. Ciber Seguridad del negocio y Ciber Seguridad de la competencia para las PYMES

Por *Hervé Falciani*

** Con la colaboración del Grupo MADphy. Instituto Universitario de Matemática Pura y Aplicada (Universitat Politècnica de València). KPI Risk Ethics & Compliance SL.*

** Hervé Falciani se dedica a aplicar las ultimas innovaciones tecnológicas a la lucha contra el fraude y es presidente de la Asociación Tactical Whistleblower, asociación sin ánimo de lucro constituida en España que nace con vocación de promover la ética y la seguridad institucional, tanto pública como privada, mediante la investigación y la aplicación de tecnologías como el blockchain.*

1. RESUMEN

En la era ciber, con el conocimiento y el aprovechamiento de las innovaciones tecnológicas, se pone en juego la fracción de poder que conformará el tejido socioeconómico más importante, el de las pymes frente a los grandes operadores de telecomunicaciones, coloquialmente llamados Telcos. Era ciber que apunta a cambios no solamente en el ámbito comercial, sino también en los ámbitos laboral y financiero, por mencionar en primer lugar los más críticos. Hay ya varios grandes grupos comerciales, a los que se van uniendo más progresivamente que aceptan el *e-cash* o las cibermonedas. El mayor mercado del mundo ya no es el mercado europeo, norteamericano o chino, sino que es Facebook o Amazon. El conocido grupo de los GAFAM, acrónimo europeo para referirse a los gigantes Google, Amazon, Facebook, Apple y Microsoft, y su exigencia de digitalizar sus relaciones comerciales, afectará directamente a las pymes. Entre otras cuestiones, les obliga cada vez con más frecuencia a ubicar sus actividades propias en la nube (en el Cloud).

Así pues, en el caso de las tiendas online, de los llamados *Market Place*, y de los pagos electrónicos, las pymes tienen que pensar en sus intermediarios comerciales y en la estrecha interacción y posición que tendrán dentro de la cadena de suministro. Esto antepone no solamente temas de preservación de la privacidad de sus clientes, sino de preservación de su marca, de sus propiedades intelectuales y comerciales mismas. Con la Libra, futura moneda de Facebook, tenemos el hilo conductor para entender los retos y las oportunidades de esos cambios que se avecinan en el ámbito ciber, entre otros, el desarrollo de nuevas formas de identificarse a través de identidades digitales.

En este capítulo valoraremos qué problemas pueden presentar para las pymes las nuevas tecnologías en la gestión de los datos durante la realización de sus actividades profesionales, ya sea a nivel operativo, financiero o regulatorio. En concreto, veremos de qué modo deben evitar ciberriesgos, y qué habilidades deben desarrollar para entregar a terceros la gestión y preservación de sus instrumentos de trabajo, de negocio y financiación, ya que ahora se verán gestionados colectivamente y por entidades especializadas y capacitadas.

En este trabajo explicaremos cuál es el estado de la cuestión en este tema, y se presentarán algunas opciones recomendables para las pequeñas y medianas empresas, especificando también cuáles son los problemas más frecuentes y algunas malas prácticas extendidas que podemos erradicar en la era de la Industria 4.0. El objetivo es explicar y evaluar los métodos más habituales en la actualidad, distinguiendo entre ellos los que pueden resultar más convenientes según el tipo de empresa para ayudar a generar valor estratégico, al tiempo que se mitigan los riesgos.

2. INTRODUCCIÓN

El sector bancario ha disfrutado de una época de supremacía en el liderazgo de la digitalización y en el uso de las últimas innovaciones en telecomunicación. Era la industria mejor posicionada para gestionar los riesgos financieros y comerciales, pero también la más expuesta a los riesgos cibernéticos.

Con la extensión de los Telcos, los riesgos cibernéticos no afectan ya sólo a las grandes empresas, de las cuales somos extremadamente dependientes, sino que, a través de nuestros sistemas conectados, como sensores o teléfonos inteligentes, por citar solo los más obvios, estamos todos expuestos, incluso a nivel privado o familiar. Esta exposición al ciberataque puede conllevar consecuencias incluso dentro de nuestro ámbito profesional. Varias empresas han visto sus sistemas informáticos comprometidos por la debilidad en ciberseguridad de sus subcontratados.

Debido al ritmo de las evoluciones tecnológicas, en muchos casos es el propio desconocimiento de las amenazas lo que representa el mayor riesgo para las empresas de cualquier tamaño. Sin embargo, debido a que las pymes no pueden dedicar el mismo volumen de recursos que las grandes empresas para protegerse contra ellos, se ha producido un considerable incremento en el número de ciberdelitos que tienen como objetivo atacar a las pequeñas y medianas empresas con consecuencias, en ocasiones, catastróficas para ellas.

No obstante, las pymes cuentan con una gran ventaja sobre las grandes empresas, que es su mayor capacidad de adaptación. Por estos motivos, creemos que es importante, en primer lugar, identificar los tipos de ciberriesgos más frecuentes y que podrían ser entregados a terceros para su gestión. De este modo, podemos conseguir que las pymes, sin necesidad de dedicar grandes recursos, puedan protegerse contra ellos.

En este sentido, se han identificado tres tipos de riesgos que al ser delegados por las pequeñas y medianas empresas podrían convertirse en oportunidades de crecimiento para ellas:

2.1. RIESGOS OPERATIVOS VS INFORMÁTICOS EN LA NUBE

El mismo Alphabet.com (grupo de Google) paga anualmente muchos millones a su concurrente Amazon para alquilar sus servicios en la nube y almacenar así servicios tales como los de Google Maps. Esto demuestra que ya incluso las más grandes empresas no gestionan ellas mismas toda la infraestructura informática que necesitan, cuando buscan la rentabilidad y la disponibilidad de sus servicios. La lista de los delitos informáticos que pueden bloquear una actividad profesional crece a diario y va más allá de los *hijacking* de su infraestructura informática, bloqueo de los datos y sistemas con *ransomware* o robo de datos.

Tradicionalmente las pequeñas y medianas compañías han alojado localmente en sus servidores el almacenamiento de los datos de gestión empresarial por dos razones fundamentales: por un lado, la necesidad de privacidad, y por otro, la disponibilidad de esos datos para asegurar la continuidad de sus servicios. El elemento común a todos ellos es el almacenamiento de la información y de los servicios y la necesidad de accesibilidad de esa misma información para poder garantizar el funcionamiento de la empresa.

En este sentido, vemos cómo la gestión y el almacenamiento seguro de la información sobre la actividad empresarial se ha convertido en los últimos años en algunos de los retos más importantes que deben afrontar las pequeñas y medianas empresas (Banham, 2017). El problema principal consiste en cómo protegerlas frente a los peligros que conlleva la digitalización de los documentos relativos a su gestión (Ribagorda-Garnacho, 2018) y el uso, cada vez más frecuente de internet.

Por este motivo, es necesario que las empresas valoren con especial atención si pueden o no externalizar sus servicios informáticos; además deberán analizar qué contenido de su información se puede filtrar y qué es lo que desean incluir en sus páginas web y en sus redes sociales como LinkedIn, ya que esta información podría ser utilizada por cibercriminales para preparar sus estafas. Se ha valorado mucho el riesgo de no controlar la información que se publica voluntariamente, pero lo que se ha estudiado mucho menos es la posibilidad de externalizar sus servicios informáticos. No obstante, en ambos casos, nos exponemos a la usurpación de nuestras identidades y mucho más, lo que conlleva graves consecuencias de naturaleza financiera pero no solo.

Los servicios en la nube presentan una oportunidad de utilización de servicios innovadores por parte de las empresas como modo eficiente para segmentar sus datos y delegar la responsabilidad de su gestión.

Por todo lo anterior, es necesario valorar detenidamente las ventajas que se derivan de la utilización de servicios en la nube, que presentan una oportunidad de utilización de servicios innovadores por parte de las empresas como modo eficiente para segmentar sus datos y delegar la responsabilidad de su gestión.

2.2. RIESGOS FINANCIEROS VS PAGO ELECTRÓNICO E IDENTIDAD DIGITAL

En el ámbito financiero, la gran mayoría de las transacciones ya no se hacen en efectivo así que, diversificando el concepto de transacción financiera o comercial, vemos que los nuevos medios de pago pueden proteger los negocios contra varias situaciones de incertidumbre.

2.2.1. Riesgo de intercambio de monedas o de falsificación

Una moneda como puede ser la Libra de Facebook permitiría disminuir el riesgo de fluctuación entre divisas. Es una de las promesas del *e-cash* y de las que han sido denominados *Stable-Coins*. Resulta obvio que la falsificación del *e-cash* es más difícil que la del efectivo.

2.2.2. Usurpación de identidad o de marca

La puesta en práctica del doble factor de autenticación, que resulta extremadamente exigente en la práctica y que requiere la inclusión de una infraestructura, mitiga el riesgo basado en la usurpación de identidad en la mayoría de los esquemas de fraude:

i. Órdenes de pago fraudulentas: Se produce cuando los delincuentes hacen que se cambien los datos de órdenes de pago que la empresa realiza con regularidad a una entidad pública o privada o a una persona física.

ii. Fraude del Director General: Se produce cuando un delincuente envía un mensaje a algún empleado de la empresa pretendiendo ser el director general y dando instrucciones para que se realice un pago.

iii. Falsificación de marca y productos.

Todos los avances en identidad digital y biometría podrán, directamente, tener un impacto en la reducción de estos riesgos en el momento en que se apliquen. En el caso de la biometría, tan solo el reconocimiento facial se considera como un negocio que se estima que verá doblar sus beneficios en los próximos cinco años hasta alcanzar los 9000 millones de dólares. Lo mismo ocurre con los pagos digitales.

2.3. RIESGOS REGULATORIOS VS TIENDA ONLINE Y INTERMEDIACIÓN

Resulta interesante considerar el caso de Amazon, que realizó más de 100.000 millones de ventas este año, y la previsión de El Corte Inglés de realizar 100 millones de transacciones con su página web. Estas cifras demuestran que las pymes se verán cada vez más forzadas a tener que dirigir sus

ventas a través de estos intermediarios, de tiendas online, ya sea a nivel operativo o regulatorio, perdiendo no sólo parte del control que tenían sobre sus clientes, sino también del que tenían sobre los medios de pago.

2.3.1. Competencia desleal y Cambio de modelo económico

El impuesto sobre los GAFAMs ilustra el cambio regulatorio que tiene que gestionar cada país.

- IVA pagado a través de las tiendas *online*

Las mayores pérdidas en la recaudación tributaria se producen con motivo de las tiendas *online* y el modo en que éstas recaudan el IVA. El Secretario de Estado francés Mounir Mahjoubi valora en alrededor de 1000 millones de euros las pérdidas anuales solo en el país. Para poderlo entender debemos sólo preguntarnos qué tipo de IVA pagamos cada vez que utilizamos tiendas *online* como, por ejemplo, Cabify, Uber, E-Booking, Amazon, etc. Mientras sean las mismas tiendas *online* las que tengan que aplicar el tipo de IVA vigente en el estado de residencia del comprador, se mantendrá una posición desleal para las pymes que no intermedien *online* su central de gestión de las ventas.

- Acceso al mercado y cláusulas abusivas

Las empresas que no conozcan las variadas ofertas de tiendas *online* estarán favoreciendo la concentración del mercado, lo que provoca posiciones monopolísticas contrarias al libre mercado que necesitan las pequeñas y medianas empresas.

- Desprestigio de la marca de sus oponentes

Debido a la existencia de posiciones monopolísticas, las empresas predominantes presionan a la competencia de modo muy extendido. Por ejemplo, se sabe gracias a la denuncia de la empresa SNAP contra Facebook[1], que existían varias actividades, presuntamente delictivas, por parte de Facebook para desprestigiar a la sociedad SNAP.

- Inteligencia económica y *e-marketing*

La misma empresa Facebook llamaba ya la atención con su aplicación Onavo que recogía de modo intensivo los datos de sus usuarios. La comercialización de la información económica y aprender a aprovecharla es cada vez un requerimiento mayor para las pymes. Al igual que las grandes empresas, las pequeñas y medianas no pueden mantenerse al margen de las ofertas en inteligencia económica y en *e-marketing,* del mismo modo que no pueden prescindir de tener una presencia cada vez más extensa en las redes sociales.

[1] El equipo legal de Snapchat recopiló durante años las maneras mediante las que Facebook trataba de frustrar a la compañía. El porfolio donde recopilaron las supuestas prácticas fue denominado 'Proyecto Voldemort', en referencia al villano contra el que se enfrenta Harry Potter. Fuente: Wall Street Journal 2019-09-24.

- Situación tributaria

En algunos países como Suiza resulta ya posible pagar los impuestos en criptomonedas. Los proyectos que están ya en marcha en varios países (*e-peso* en Uruguay, la que proyecta el Banco Central de China) invitan a considerar qué consecuencias puede tener todo ello para las economías locales.

- Reputación y e-reputación

Resulta fundamental obtener información exacta relevante sobre sus clientes e intermediarios antes de iniciar relaciones. La obtención de datos independientes sobre su situación tecnológica, financiera y hábitos de pago, puede evitar que su empresa incurra en grandes pérdidas.

- Limitación judicial de las exportaciones

Gestionar su negocio de modo digital permite un acceso y un análisis a medida, caso por caso y en tiempo real de información relevante.

2.3.2. Posibles soluciones frente a los desafíos

Entre las pymes, los problemas más comúnmente identificados para la adopción de estos mecanismos, y que con frecuencia son fuente de preocupación y por ello dignos de mención son dos: en primer lugar, la sobreestimación de la dificultad técnica de la externalización de sus instrumentos de trabajo y negocio, reduciendo la calidad del resultado por falta de dedicación seria al problema; y, en segundo lugar, la posible existencia de problemas legales sobre la privacidad de ciertos datos y el almacenamiento de información de baja calidad por falta de criterios de selección claros.

Algunos ejes principales sobre los que deberían girar las posibles soluciones a estos problemas y a otros de tipo más práctico, relacionados con los soportes concretos para la gestión del almacenamiento de los datos, son los siguientes:

i. Selección efectiva de datos para minimizar el volumen del conjunto de aquellos datos que deben guardarse.

ii. Desvinculación de los datos del sujeto referente mediante el uso de identidades digitales.

iii. Adopción de algunos cambios conceptuales referentes a la privacidad de datos y almacenamiento, para adaptarse a las nuevas circunstancias de seguridad en el contexto Big Data: *blockchain*.

Trataremos estos tres puntos en la siguiente sección, proponiendo reglas de uso y elementos para contrastar sus ventajas e inconvenientes, además de introducir algunos elementos nuevos que también afectan a la ciberseguridad comercial de las pymes.

3. EJES DE ACTUACIÓN PARA OPTIMIZAR SU ENTORNO LABORAL

3.1. GESTIÓN DE LOS DATOS EMPRESARIALES

Hemos sintetizado en los siguientes tres apartados los elementos importantes a tener en cuenta en relación con la gestión de los datos empresariales. Debe entenderse que el enfoque de nuestro análisis no es exhaustivo, y que lo que se pretende es poner el foco sobre algunos puntos especialmente sensibles; según el perfil empresarial, aparecen problemas y situaciones que deben ser tratadas desde la especificidad del sector y resolverse según las herramientas adecuadas en ese ámbito, sea industrial, financiero o de servicios.

3.1.1. Principio de economía en el almacenamiento de los datos

Posiblemente, entre las medidas más simples a adoptar por parte de las pequeñas y medianas empresas, podemos destacar un principio básico de economía en la gestión de datos, que consiste en guardar solo los datos valiosos y desechar los datos de segundo nivel o intrascendentes, cuidando la homogeneidad de formato para facilitar su uso, y paliar así en lo posible la falta de recursos específicos para la gestión.

Se trata de aplicar la navaja de Ockham al problema, es decir, un método de reducción de los datos almacenables, eliminando sistemáticamente aquello que, aunque pudiera ser inicialmente considerado como complementario, en realidad no es necesario. Resulta imprescindible mantener los principios de economía ecológica para afrontar el problema: no gastar en recursos más que lo estrictamente necesario, aplicando el sentido común para fijar aquellos contenidos realmente indispensables que se deban preservar. Es lo que en inglés se denomina *sparsity*, que podría traducirse como “principio de parquedad”; esto es, solo deben almacenarse aquellos datos estrictamente necesarios para asegurar que se preserva la posibilidad de recuperación de toda la información realmente relevante. En la actualidad existen algunos algoritmos que pueden hacer esto de forma automática dependiendo del tipo de datos. Los sistemas basados en Inteligencia Artificial pueden servir para ese fin, ya que son capaces de seleccionar e identificar los datos verdaderamente relevantes.

3.1.2. Identidades digitales y privacidad

Como hemos indicado antes, otro eje fundamental para la actuación puede ser la utilización de lo que se han denominado identidades digitales - *digital ID* - (Sullivan, 2018), que constituyen un escudo para la protección de los datos (Friedman and Wagoner, 2015). Se basa en desvincular los datos en sí de los sujetos a los que se refieren, tanto si son personas, empresas o entidades públicas, o bien otro tipo de agentes económicos.

En este contexto, la pregunta que surge es: si utilizamos exclusivamente identidades digitales, ¿podemos trabajar sin conocer al cliente? En cualquier caso, ésta podría ser una solución adecuada, aunque serían necesarios cambios radicales en los procedimientos.Está claro que se puede bajar el nivel de exposición a la cibercriminalidad disminuyendo el intercambio de datos personales entre proveedores y clientes.

De manera complementaria a los cambios de procedimiento necesarios para que las empresas puedan trabajar en este contexto, resulta relevante que se consoliden los cambios legislativos y normativos indispensables para asegurar los derechos de los particulares al respecto de los datos digitales que les afectan, tanto a nivel nacional como europeo.

3.1.3. Otras formas de entender el almacenamiento de datos para reducir el riesgo de posición monopolístico de las tiendas *online*: el uso de sistemas descentralizados como el *blockchain*.

Otro elemento fundamental de almacenamiento de la información económica en la actualidad es *blockchain*, que consiste básicamente en una red de usuarios que constituye un sistema para el registro de información, fundamentalmente de tipo transaccional, que es inmutable porque está certificado por un sistema verificado por múltiples agentes y sucesivamente encriptado, de forma que todos los elementos de información, una vez fijados, permanecen en todos los ordenadores que forman la red. Así, todos los pagos y transacciones quedan almacenados, aunque dejan de ser de acceso exclusivo para el que los introduce.

Es necesario participar en una entidad colaborativa y, por lo tanto, hacer uso de ciertos conocimientos propios de la empresa o contratarlos. El resultado es que se sustituye la privacidad de los datos por la trazabilidad de esos mismos datos, situando la motivación por la cual se pretende el almacenamiento en un contexto diferente, en el que lo privado, referido a los datos, tiene otro sentido. El lector interesado puede encontrar en Reyna *et al* (2018) y Taylor *et al* (2019), y las referencias que aparecen en el segundo trabajo, información sobre el uso de blockchain en el campo de la ciberseguridad.

3.2. EJEMPLOS DE DESCENTRALIZACIÓN EN EL ALMACENAMIENTO DE LOS DATOS

Las entidades bancarias, los gestores externos que trabajan para las pymes, así como otros agentes involucrados en la actividad económica de las mismas y que en la realización de esa actividad manejan los datos de éstas, pueden a su vez ser los agentes que almacenen los datos que ellos gestionan. No es necesario que las empresas tengan copias de ese material pues se puede delegar en estos agentes su conservación en base a un proceso de externalización basado en la confianza. Las entidades seleccionadas para ese objetivo (por ejemplo, los bancos) a menudo tienen recursos para tales fines pudiendo hacerse cargo de este material.

Para bajar el nivel de exposición al ciberriesgo, se puede reducir la cantidad de datos digitales gestionados, lo que evitaría el riesgo que representa la información duplicada. Esto puede conseguirse aplicando la compartimentación en el almacenamiento; es decir, separando los datos a guardar por áreas, siguiendo, por ejemplo, este esquema:

a) Gestión de los ingresos: la institución bancaria con la que se trabaje, que tiene generalmente muchos recursos dedicados a la ciberseguridad, puede encargarse del almacenamiento de los datos. Si los pagos de los clientes se hacen con tarjeta, por ejemplo, podrían ser gestionados directamente por el banco.

b) Contabilidad, facturación: los datos contables pueden pasar a ser responsabilidad del gestor económico, un agente muchas veces externo a la empresa.

c) Datos transaccionales: aunque tradicionalmente han sido responsabilidad de los bancos, el uso de nuevas formas de pago de las empresas -por ejemplo, mediante criptomonedas- pueden trasladar esta responsabilidad de nuevo a la empresa. En este caso pueden ser almacenados mediante *blockchain*.

Se está tomando muy en serio este tema. El ultimo G7 puso en marcha varias iniciativas para acompañar el desafío que representan las cibermonedas a nivel de la economía mundial. Entre ellas, se ha configurado un grupo de trabajo sobre el *e-cash* y en particular sobre la Libra, la moneda de Facebook, y los *Stable-Coins*, liderado por el señor Benoit Coeure, miembro del comité ejecutivo del Banco Central Europeo. Hoy, según datos de la Universidad de Cambridge, Facebook está siendo utilizado por 2400 millones de individuos. Otro dato relevante es el extraído de coinMarketCap, plataforma creada para realizar un seguimiento de la capitalización de diferentes criptomonedas, según la cual, el uso de las criptomonedas se ha multiplicado por 100 en menos de cinco años, mientras solo concierne a una población de alrededor de 35 millones de personas.

4. EJES DE ACTUACIÓN PARA UNA GESTIÓN ALTERNATIVA DE SUS INFORMACIONES FINANCIERAS

Desde el punto de vista legal, y frente a sus clientes, las instituciones financieras tienen la responsabilidad de responder a la creciente necesidad de asegurar sus datos. Se pretende que los datos relativos a esa gestión sean accesibles, pero cumpliendo con la obligación impuesta por la directiva europea sobre medios de pago (PSD2), de ofrecérselo sólo a los agentes autorizados, pero comprometiéndose a facilitar la consulta de los mismos a los interesados, siempre y cuando se garantice que cualquier cliente o técnico pueda verificar esa información.

En este balance entre la accesibilidad y la seguridad es donde se puede abrir la brecha que tanto preocupa a los empresarios: el acceso ilícito a sus datos. Este acceso puede producirse por múltiples razones, que van desde el espionaje industrial hasta, por ejemplo, la exposición pública de datos confidenciales para cuestionar a la propia empresa, con el fin de desacreditarla frente a sus clientes (Jang-Jaccard y Nepal, 2014).

4.1. PROTECCIÓN Y OBJETIVACIÓN DEL PERFIL FINANCIERO

En esta situación, que preocupa no solo a instituciones financieras, se han propuesto soluciones un tanto extremas, pero que dan una idea de la gravedad del problema: por ejemplo, algunos bancos (¡suizos!) han llegado a proponer volver al almacenamiento de los datos más sensibles en papel, para evitar en lo posible el acceso no autorizado y masivo a sus datos confidenciales en el país que se considera a sí mismo: ¡la *criptonación* más avanzada!

Gestionar los datos más críticos gracias a soportes físicos, en oposición a la utilización de soportes digitales, es una de las 'innovaciones' que han surgido de las criptomonedas y que es conocido como el *Hard-wallet*. Consiste exactamente en lo que proponen algunos bancos suizos: utilizar papel para almacenar las contraseñas.

Otra idea que no es extrema y que ya se ha concretado en proyectos muy relevantes es el uso de la tecnología *blockchain* (en español, cadena de bloques) que puede facilitar también sistemas de almacenamiento asociados (Kshetri, 2017), a pesar de que es posible que conlleve algunos problemas de tipo legal (Millard, 2018), principalmente por la falta de regulación clara de su uso para asuntos financieros.

Y una tercera opción propuesta es que, en la digitalización, los datos queden sólo asociados a identidades virtuales (ID digital), sin referencia nominativa. Estas dos últimas opciones, por ser más asequibles, están siendo consideradas por pymes que cuentan con menos recursos para gestionar sus datos.

4.2. DATOS ALTERNATIVOS Y FINANCIACIÓN DE LA CADENA DEL SUMINISTRO

Ofrecer un nuevo modelo de gestión de su privacidad permite compartir de modo trazable y 'no-repudiable' las transacciones comerciales. Con registros que pueden ser públicos, los registros distribuidos (DLT y *blockchains*), las empresas encuentran un ámbito natural para incentivar la financiación de su cadena de suministro (*Supply Chain Finance* y *Revers Supply Chain Finance*). Los instrumentos de financiación usuales, incluyendo los más antiguos -créditos documentarios o cuentas abiertas- tienen ahora una alternativa más transparente y más eficiente con los sistemas distribuidos y semipúblicos. Es un avance que permite agilizar y bajar el coste de financiación en un mercado de créditos abiertos y perfiles financieros accesibles prácticamente en tiempo real.

Es un eje de investigación muy prometedor, en el cual participan tanto actores públicos como privados. En varias comunidades autónomas se han puesto en marcha iniciativas en este sector, y en la valenciana, por ejemplo, se puede nombrar como instituciones interesadas en el tema al Instituto Universitario de Matemática Pura y Aplicada (IUMPA) o a la Agencia Valenciana Antifraude.

En estas iniciativas es necesario que haya una pluridisciplinariedad y que se cuente con la colaboración de expertos en derecho, filología, datos abiertos, sistemas distribuidos y matemática aplicada, entre otras disciplinas. Las experiencias que se derivan de esta pluridisciplinariedad, unidas a la Inteligencia Artificial o a otras condiciones formales, resultan imprescindibles para garantizar la veracidad o certeza de la información. Gracias a la ciencia de los datos (*Data Science*), se con-

sigue a través de los datos alternativos ratings con una calidad muy superior a los usuales. Son condiciones que, aquellas pymes que sepan aprovecharlas, se situaran muy favorablemente en la obtención de la tesorería que requieren sus negocios.

Como hemos mencionado con anterioridad, la gestión de la información y de los datos siempre ha sido un elemento fundamental para garantizar el buen funcionamiento de las empresas, pero ahora más que nunca, ya que cualquier debilidad en ese ámbito de gestión será aprovechada por ciberdelincuentes para cometer sus fraudes y estafas. Por ello, resulta muy importante que se contrapongan los riesgos a las oportunidades correspondientes.

5. EJES DE ACTUACIÓN PARA REDIRIGIR SU EXPOSICIÓN A LOS RIESGOS REGULATORIOS

En la actualidad sabemos que las pymes están siendo con más frecuencia víctimas de ciberataques debido a que son consideradas objetivos más fáciles. Por este motivo, resulta necesario tener en cuenta varias cuestiones relevantes. La primera, la responsabilidad ineludible de las empresas para con sus clientes en lo que respecta a la gestión de sus datos, motivo por el que resulta imperativo que se introduzcan todos los recursos que sean necesarios para defender la seguridad de los datos de sus clientes y de la gestión de su negocio. En el supuesto de que las pequeñas y medianas empresas decidieran guardar los datos usando sus recursos informáticos propios, deberían tener en cuenta que, en el supuesto de que sus servidores fueran asaltados por piratas informáticos, la empresa será responsable de los perjuicios causados, lo que podría dañar considerablemente su reputación.

Asimismo, la violación de los principios éticos mínimos sobre la gestión de datos de carácter personal de sus clientes afectaría, no sólo a su reputación, sino que además este error, voluntario o no, podría ser constitutiva de delito.

En este contexto, el registro de los intercambios con los clientes mediante blockchain permitiría preservar la información de los ataques no sólo de los *bots*, sino también de ciberataques de todo tipo y procedencia. En muchas ocasiones, con respecto a los datos personales, puede convenir aplicar el concepto de 'NO' KYC (negación de las siglas en inglés de la expresión "Conozca a su Cliente"), que puede sintetizarse en el lema "si no lo necesitas, elimínalo", y que consiste en la aplicación del siguiente simple argumento: si no tienes datos personales, no necesitas protegerlos.

Por último, frente al concepto tradicional de privacidad, es posible que sea la trazabilidad la verdadera transparencia en la gestión de los datos de empresa, porque no expone a la compañía al riesgo de apropiación por agentes externos porque de alguna forma ya son públicos y están protegidos por la propia estructura del *blockchain* que escuda de posibles apropiaciones fraudulentas por parte de la competencia.

6. CONCLUSIONES

Hoy en día existen múltiples empresas especializadas en prestar ayuda a las pymes para que éstas cuenten con aliados estratégicos en el ámbito de la transformación digital. El primer principio que en nuestra opinión debe siempre tenerse en cuenta es el de la máxima simplificación de los registros a conservar.

Debe seleccionarse cuidadosamente qué información merece ser almacenada para disminuir el volumen de información y que así sea más fácil su gestión. No es necesario que toda la información esté centralizada. Se recomienda transferir la salvaguarda de los datos, según su tipo, a otros agentes para externalizar su almacenamiento.

En lo que respecta a los datos de registro de transacciones comerciales, si el soporte que se usa está basado en la tecnología *blockchain*, que tiene como garantía de validez el carácter consensual de su funcionamiento, está asegurada no sólo la veracidad de sus contenidos, sino que su autenticidad sea fácilmente demostrable, como consecuencia de la propia estructura del sistema de almacenamiento. Esto puede utilizarse para ganar la confianza de los clientes/usuarios, lo que afecta positivamente al prestigio de la empresa. *Blockchain* facilita también la interactuación y la colaboración entre distintos agentes, y minimiza el riesgo de exposición a los ciberataques de los actores intermedios en la cadena, protegiendo no sólo de la sustracción de datos, sino también de sus consecuencias.

7. BIBLIOGRAFÍA

Banham, R. (2017). Cybersecurity threats proliferating for midsize and smaller businesses. *Journal of Accountancy, 224(1).*

Friedman, A. R., & Wagoner, L. D. (2015). The need for digital identity in cyberspace operations. Journal of Information Warfare, 14(2), 41- 51.

Garnacho, A. R. (2018). Panorama actual de la ciberseguridad. *Economía industrial, 410,* 13-26.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993.
https://doi.org/10.1016/j.jcss.2014.02.005

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*(10), 1027-1038.
https://doi.org/10.1016/j.telpol.2017.09.003

Millard, C. (2018). Blockchain and law: Incompatible codes?. *Computer Law & Security Review, 34*(4), 843-846.
https://doi.org/10.1016/j.clsr.2018.06.006

Sullivan, C. (2018). Digital identity–From emergent legal concept to new reality. *Computer Law & Security Review, 34*(4), 723-731.
https://doi.org/10.1016/j.clsr.2018.05.015

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88, 173-190.
https://doi.org/10.1016/j.future.2018.05.046

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2019). A systematic literature review of blockchain cyber security. Digital Communications and Networks.
https://doi.org/10.1016/j.dcan.2019.01.005

Diarios electrónicos

Wells, Georgia and Seetharaman, Deepa (24 de septiembre de 2019). Snap Detailed Facebook's Aggressive Tactics in 'Project Voldemort' Dossier. *The Wall Street Journal*. Recuperado de https://www.wsj.com/articles/snap-detailed-facebooks-aggressive-tactics-in-project-voldemort-dossier-11569236404

Normas jurídicas

Directiva (UE) 2015/2366 del parlamento europeo y del consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior. https://www.boe.es/doue/2015/337/L00035-00127.pdf

CAPÍTULO VI

ANÁLISIS DEL COMPORTAMIENTO DE USUARIOS DE ORDENADORES, INCIDENTES DE SEGURIDAD Y FRAUDE MEDIANTE EL USO DE *SELF-ORGANIZING MAPS*

VI. Análisis del comportamiento de usuarios de ordenadores, incidentes de seguridad y fraude mediante el uso de *Self-Organizing Maps*

Por José M. Martínez-Martínez[1], Julio Navío-Marco[2], Alberto Urueña-López[3], Emilio Soria-Olivas[1]

- [1]*IDAL, Intelligent Data Analysis Laboratory, Departamento de Ingeniría Electrónica, Escuela Tècnica Superior d'Enginyeria , Universitat de València.*

- [2]*Facultad CC de Económicas y Empresariales, Departamento de Organización de Empresas, Universidad Nacional de Educación a Distancia (UNED).*

- [3]*Departamento de Administración de Empresas, Escuela Técnica Superior de Ingenieros Industriales, Universidad Politécnica de Madrid.*

1. INTRODUCCIÓN

El crecimiento del uso de internet y la cantidad de programas y aplicaciones descargados ha sido exponencial en los últimos años. Sin embargo, aparecen nuevos peligros a medida que aumenta la cantidad de ventajas. La seguridad informática surge en este entorno para proporcionar protección contra esos riesgos. También conocida como ciberseguridad, puede definirse como la seguridad aplicada a dispositivos como a ordenadores y teléfonos inteligentes, así como a redes informáticas. El campo incluye todos los procesos y mecanismos por los cuales el equipo informático, la información y los servicios están protegidos contra el acceso, cambio o destrucción no intencionados o no autorizados, y es de creciente importancia debido a la progresiva dependencia de los sistemas informáticos en la mayoría de las sociedades. Esto incluye seguridad física para evitar el robo de dispositivos y seguridad de la información para proteger los datos en esos dispositivos. La seguridad cibernética también es esencial para mantener la integridad de la información del usuario. Estos conceptos cobran especial relevancia con el crecimiento exponencial de los dispositivos conectados (*internet of Things*, IoT).

La percepción de peligro en los usuarios es un punto clave en el uso de nuevas tecnologías, ya que el sentimiento de desconfianza puede retrasar la adopción de dichas tecnologías. Por lo tanto, es crucial monitorear los sentimientos y sensaciones de los usuarios sobre los riesgos asociados con las nuevas Tecnologías de la Información y las Comunicaciones (TIC) mientras se prueba si esos sentimientos son fundados.

Los usuarios de ordenadores que se involucran en conductas de riesgo han llamado la atención de los equipos investigadores porque se les considera uno de los eslabones débiles en el campo de la Sociedad de la Información. La literatura sobre la toma de riesgos va más allá del dominio del usuario del ordenador, y la evidencia empírica disponible ha demostrado las consecuencias negativas de los comportamientos de riesgo. En el lado opuesto, la comunidad de usuarios de comercio electrónico tiene una mayor percepción del riesgo. Por ejemplo, un cliente de comercio electrónico tiene una mayor conciencia de riesgo sobre una transacción en términos de pago y entrega que cuando realiza una transacción tradicional en una tienda física.

Este capítulo realiza un diagnóstico del estado de la seguridad cibernética en los hogares digitales españoles, analizando la adopción de medidas de seguridad y el nivel de incidencia de situaciones que pueden constituir riesgos de seguridad. Este estudio es similar a otros ya realizados. Sin embargo, dos de las principales diferencias en este documento son: (i) la confianza de los usuarios domésticos también se evalúa mediante un análisis informático, que determina el grado de infección de *malware*, y (ii) la herramienta utilizada para llevar a cabo el análisis mencionado arriba son los Mapas Auto-Organizados (SOMs, de sus siglas en inglés *Self-Organizing Maps*), un poderoso método de minería de datos visuales que proporciona una representación de baja dimensión de datos de alta dimensión, mejorando así la visualización y la capacidad de interpretación para el reconocimiento de patrones complejos.

2. *SELF-ORGANIZING MAPS*

2.1. ASPECTOS TEÓRICOS

Los Mapas Auto-Organizados son una de las herramientas de visualización más populares hoy en día. El SOM es una red neuronal artificial (RNA), propuesta por Teuvo Kohonen en el año 1982 y, desde entonces, ha sido analizada y utilizada ampliamente. Una RNA es un modelo computacional inspirado en los conceptos básicos del funcionamiento del cerebro humano. En general, una RNA emplea conexiones entre sus unidades de procesamiento -llamadas neuronas- para almacenar los conocimientos necesarios para realizar una tarea específica. La característica fundamental de una RNA es la capacidad de aprender del medio ambiente y mejorar su rendimiento de acuerdo a un modelo prescrito que constituye el paradigma de aprendizaje.

A diferencia del SOM, las técnicas clásicas solamente pueden manejar visualizaciones precisas de conjuntos de datos completos cuando el número de características requeridas es igual o inferior a tres; para representar un mayor número de características, solamente se pueden llevar a cabo proyecciones en tres dimensiones, estableciendo restricciones -como mantener fijo un cierto con-

junto de variables y representar el resto-. Tal restricción conduce a una representación parcial de la información. Además, la mayoría de los conjuntos de datos reales están formadas por más de tres características, haciendo difícil su representación gráfica. Para ese tipo de representación, es decir, una visualización completa de todas las variables sin restricción que hará posible encontrar patrones en conjuntos de datos con alta dimensionalidad, los Mapas Auto-Organizados (SOM) están especialmente indicados.

En particular, el SOM opera para producir una representación de baja dimensión (típicamente 2D) de datos de alta dimensión mediante la identificación de datos similares en el espacio de entrada, y agrupándolos en una cuadrícula. La característica más atractiva de SOM es que las matemáticas subyacentes aseguran que el mapa es una representación fiel de los datos originales, por ejemplo, dos puntos de datos se representan cerca uno del otro en el mapa resultante cuando tienen características similares. Esto es, el SOM mantiene una relación de vecindad entre el espacio original de los datos N-dimensionales y de la red (o cuadrícula) de baja dimensionalidad (en la que se efectúa la visualización). En nuestro caso, esto significa que usuarios que muestran un comportamiento similar -descrito por las variables que describen el problema- estarán localizados en zonas cercanas en la red de baja dimensión mencionada anteriormente.

El SOM, al igual que las RNAs, se compone de unidades de procesamiento (neuronas), organizadas en una red o cuadrícula de baja dimensión, normalmente en dos dimensiones. El número de neuronas puede variar desde unas pocas docenas hasta varios miles. Cada neurona está representada por un vector de pesos $m=\left[m_1,\ldots,m_d\right]$, donde d es igual a la dimensión de los vectores de entrada.

En el diseño de los Mapas Auto-Organizados hay que tener en cuenta diferentes parámetros. La primera opción está relacionada con la selección del tipo de mapa -hexagonal o neuronas rectangulares-, y también con el número de neuronas seleccionadas, ya que esto va a definir el tamaño de la red de baja dimensionalidad. Esta elección dependerá del número de patrones considerados (número de usuarios), el número de variables que definen estos patrones y, por último, de la dispersión presente en los datos.

El siguiente paso es obtener los coeficientes asociados a cada neurona (vector d-dimensional **m** mencionado anteriormente), llamados pesos sinápticos. Para tal fin se utiliza un algoritmo de aprendizaje. El primer paso de este algoritmo es la inicialización de los pesos, lo que permite un gran número de posibilidades. Una vez que los valores iniciales de los pesos sinápticos han sido seleccionados, el siguiente paso es acercarlos a los valores óptimos por medio de un procedimiento iterativo. En cada etapa de entrenamiento, se elige al azar un vector de muestra *x* seleccionado del conjunto de datos de entrada, y se calculan las distancias entre éste y todos los vectores de pesos (pesos sinápticos) del SOM utilizando alguna medida de distancia. La neurona cuyo vector de pesos es más cercano al vector de entrada x se denomina Unidad Más Similar (o BMU de sus siglas en inglés *Best-Matching Unit)*, denotado a continuación por *c*:

$$\left\|x-m_c\right\|=\min_i\left\{\left\|x-m_i\right\|\right\}$$

donde $\| \ \|$ es una medida de distancia, típicamente distancia euclídea, la cual viene dada por:

$$\|x-m\|^2 = \sum_{k \in K}^{M} (x_k - m_k)^2$$

donde *K* es el conjunto de variables conocidas del vector de muestra *x* y x_k y m_k son las *k*-ésimas componentes de los vectores de muestra y de peso, respectivamente.

Después de encontrar la BMU, los vectores de pesos del SOM se actualizan de forma que la BMU se acerca al vector de entrada en el espacio de entrada. Los vecinos topológicos de la BMU son tratados de manera similar. Este procedimiento de adaptación "arrastra" la BMU y sus vecinos topológicos hacia el vector de muestra como se muestra en la figura 1.

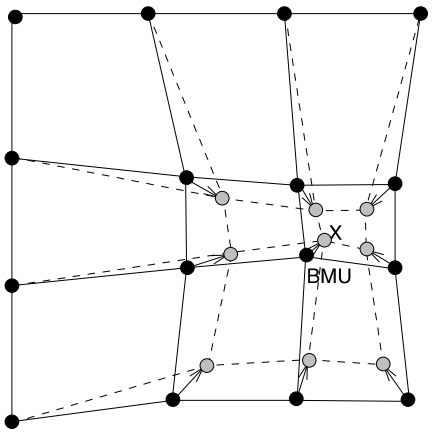


Figura 1. Actualización de la Best Matching Unit (BMU) y sus vecinos hacia la muestra de entrada marcada con x. Las líneas continuas y discontinuas corresponden a la situación antes y después de la actualización, respectivamente. Fuente: Elaboración propia.

La regla de actualización de SOM para el vector de pesos de la unidad *i* es:

$$m_i(t+1) = m_i(t) + \alpha(t) \cdot h_{ci}(t) \cdot \left[x(t) - m_i(t) \right]$$

donde *t* denota tiempo. La *x(t)* es un vector de entrada extraído al azar de los datos de entrada en el momento *t*, *hci(t)* el *kernel* de vecindad alrededor de la unidad ganadora *c* y α(t) la tasa de aprendizaje en el instante *t* (ver Figura 2). El *kernel* de vecindad es una función no creciente del tiempo y de la distancia de la unidad i de la unidad ganadora c. Este define la región de influencia que tiene la muestra de entrada en el SOM.

El entrenamiento se realiza generalmente en dos fases. En la primera fase se utiliza una tasa de aprendizaje inicial y un radio de vecindad relativamente grande. En la segunda fase tanto la tasa de aprendizaje, como el radio de vecindad, son pequeños desde el principio. Este procedimiento

corresponde a empezar ajustando el SOM aproximadamente al mismo espacio que los datos de entrada y luego afinar el mapa. Una vez que el entrenamiento del mapa ha terminado, la visualización del mapa bidimensional proporciona información cualitativa acerca de cómo las variables de entrada están relacionadas unas con otras para el conjunto de datos utilizado para entrenar el mapa.

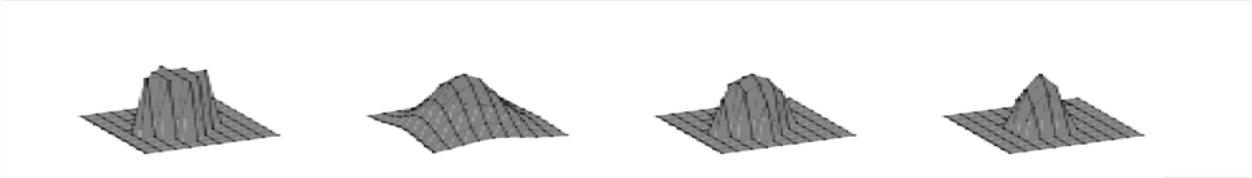


Figura 2. Diferentes funciones de vecindad. Desde la izquierda 'bubble', 'gaussian', 'cutgauss', 'ep'. Fuente: Elaboración propia.

En resumen, las características principales del SOM son:

- El mapeo llevado a cabo por el SOM no es lineal, mucho más potente que los métodos lineales clásicos.
- El SOM tiene la capacidad de preservar relaciones topológicas; es decir, patrones de entrada que son similares en el espacio original de alta dimensión de los datos son mapeados cerca en el plano de componentes proporcionados por la visualización del SOM.

2.2. VISUALIZACIÓN DEL SOM

PLANO DE COMPONENTES

Después del proceso de entrenamiento de un SOM, es muy sencillo proyectar el mapa en las diferentes características; estas proyecciones se conocen como planos de componentes, también conocidas como mapas de componentes. Los planos de componentes pueden ser representados en un gráfico, de manera que la información de cada variable puede ser visualizada permitiendo una visualización más completa de la realidad. Esto hace posible la detección de las relaciones entre las diferentes variables analizadas. Un plano de componentes de un SOM es un mapa en el que, para cada neurona, solamente se representa una componente de su vector de pesos (correspondiente a una variable de entrada dada); de este modo, en los experimentos se puede visualizar un total de N planos de componentes (donde N es la dimensión de los datos o el número de variables). Por lo tanto, los patrones de entrada que son mapeados en una cierta área de un plano de componentes

mantienen las posiciones gráficas en todos los otros planos de componentes. Dado que todos los planos de componentes en realidad pertenecen al mismo mapa, se puede analizar una cierta zona del mapa para las diferentes características al mismo tiempo.

En el plano componentes *i*, cada neurona en la red (cuadrícula) del SOM se colorea en base al valor de la componente *i*-ésima de su vector de pesos. Los valores más altos se representan generalmente en tonos rojos y los inferiores en tonos azules. Por lo tanto, los planos de componentes tienden a mostrar algunas partes del mapa con un color similar; esto significa que vectores de entrada similares se agrupan en esas partes concretas del mapa, es decir, las neuronas del mismo color dentro de un plano representan un conjunto de vectores de entrada que son similares de acuerdo a esa variable específica. La misma región dentro de cada plano (por ejemplo, la esquina superior izquierda) identifica el mismo conjunto de patrones de entrada (en nuestro caso usuarios), pero cada plano se centra en una variable diferente.

Este tipo de visualización permite comparar los valores a través de diferentes características (variables): por ejemplo, se podría identificar fácilmente las regiones del espacio de entrada donde una variable i_1 posee valores grandes (región de color rojo en el plano i_1), mientras que la variable i_2 posee valores pequeños (región azul en el plano i_2 - correlación negativa). Por lo tanto, la comparación entre diferentes planos permite una comprensión intuitiva de las relaciones existentes entre las variables bajo estudio. Mientras que otras representaciones clásicas necesitan establecer algunos umbrales para enfatizar diferentes perfiles, el SOM puede trabajar con variables continuas de manera que los perfiles se muestran con un degradado de color, como se ha mencionado anteriormente. Cada plano de componentes se muestra junto a una barra de color que da información sobre la relación entre el color y el valor numérico correspondiente.

MAPA DE GANADORAS

Un 'mapa de ganadoras', también conocido como 'mapa de BMU (*Best Matching Unit*)', representa la respuesta de los datos en los Mapas Auto-Organizados. Normalmente, dicha respuesta se muestra en el mapa usando las BMUs, por lo que el mapa presentado tiene el mismo tamaño que los planos que componen del SOM. El 'mapa de ganadoras' viene representado por marcadores que muestran el número de veces que cada unidad del mapa, o neurona, fue la BMU (unidad más similar) para cada registro de entrada. De este modo, se representa la distribución de las mejores unidades (unidades ganadoras o BMUs) para un determinado conjunto de datos, y por lo tanto las regiones del SOM que contienen más datos.

La figura 3 muestra un ejemplo de un 'mapa de ganadoras' convencional, donde cada neurona está representada por un hexágono en la cuadrícula del mapa. El área coloreada de negro dentro de cada hexágono es proporcional al número de patrones de entrada que son más similares a esta neurona. Esto da una idea cuantitativa del número de vectores de entrada que pertenecen a cada neurona, de modo que las neuronas más grandes alojan la mayor parte de los registros, mientras que las más pequeñas denotan las regiones del SOM que poseen menos registros, pero no por ello menos importantes. En algunos casos, las áreas del mapa representadas por un número pequeño de vectores de entrada no se deben descuidar si el objetivo está relacionado con la extracción de

conocimiento e identificación de grupos minoritarios como, por ejemplo, usuarios que sufrieron fraude, donde el objetivo es identificar los perfiles de dichos usuarios. En este caso, se debe tener en cuenta que el número de usuarios analizados de este tipo es bajo, y no representan un perfil de usuario estándar.

De este modo, el 'mapa de ganadoras' respalda y apoya la interpretación de los planos de componentes, ya que resalta aquellas regiones que en su mayoría son dignas de atención en la búsqueda de correlaciones entre planos. Además, se puede dibujar en diferentes colores varias 'neuronas ganadoras'. Esto hace posible comparar los diferentes patrones asociados a diferentes clases -en un problema supervisado- por la distribución de sus 'ganadoras' en el mapa. Como se muestra en los resultados, estos mapas proporcionan más información que los obtenidos mediante un etiquetado simple o de un solo color, ya que podemos distinguir entre las diferentes clases o grupos presentes en el problema.

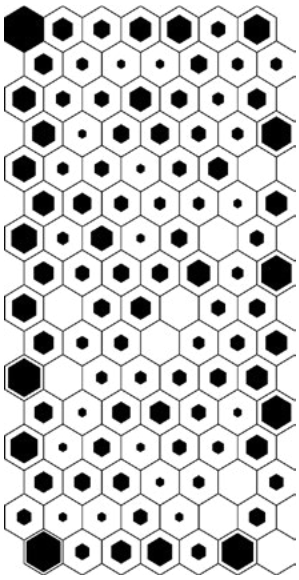


Figura 3. Ejemplo de un "Mapa de ganadoras" convencional, donde cada neurona se representa por un hexágono en la rejilla del mapa. El área coloreada dentro de cada hexágono es proporcional al número de patrones de entrada que mejor representados son por dicha neurona. Fuente: Elaboración propia.

3. MATERIAL

Esta sección abordará la descripción de los detalles de los cuestionarios y datos utilizados para entrenar los SOMs.

3.1. CUESTIONARIO

Los datos fueron extraídos de encuestas bimensuales y trimestrales que abarcan desde diciembre de 2013 hasta junio de 2014 en España y fueron obtenidos por el Observatorio Nacional de Telecomunicaciones y Sociedad de la Información del Ministerio de Industria español. Las encuestas se realizaron a través de cuestionarios *online* de un panel de usuarios de internet a quienes se les pidió que los completaran por sí mismos. Las encuestas fueron dirigidas a usuarios españoles con al menos un acceso mensual a internet desde casa. El diseño de la muestra tuvo en cuenta una estratificación proporcional por tipo de hábitat para cada región española. Las cuotas del segmento social y el número de personas en el hogar se consideraron para ese fin. Se realizó una prueba previa con 50 usuarios y no se encontraron incidentes, por lo que el cuestionario para el presente estudio fue aprobado. Primero, se le pidió al usuario que respondiera preguntas que describieran su perfil (variables demográficas, sistema operativo, navegador, etc.). El resto de la encuesta se dividió en ocho módulos diferentes, que miden diferentes aspectos:

- Módulo A: Uso de internet. Mide el uso de varios servicios ofrecidos en internet, por ejemplo, seleccionar de una lista todos los servicios de internet que se utilizaron en el último trimestre.

- Módulo B: Medidas y hábitos de seguridad en internet. Mide las acciones de los usuarios con respecto a la seguridad de internet, por ejemplo, seleccionar medidas de seguridad o herramientas de *software* que se utilizaron en el último trimestre o con qué frecuencia los usuarios escanean su sistema o buscan actualizaciones de antivirus.

- Módulo C: Incidentes de seguridad. Contiene preguntas sobre incidentes de seguridad experimentados por los usuarios en sus ordenadores, por ejemplo, infecciones de *malware*/*adware* o virus sufridas en el último trimestre y su gravedad.

- Módulo D: Fraude. Contiene preguntas relacionadas con el fraude experimentado por los usuarios relacionado con *phishing* o compras *online* (productos no recibidos o falsificados).

- Módulo E: Seguridad de teléfonos inteligentes. Mide las acciones de los usuarios con respecto a la seguridad de los teléfonos inteligentes, tales como descargas de aplicaciones o servicios de internet utilizados, copia de seguridad de información importante, uso de contraseñas o números PIN, etc.

- Módulo F: Seguridad Wi-Fi. Mide las acciones de los usuarios con respecto a la seguridad de Wi-Fi, como conexión a redes *wifi* públicas y protocolos inalámbricos utilizados.

- Módulo G: Opinión. Mide la opinión del usuario sobre la confianza en internet, como valorar cuanto de seguro se siente el usuario cuando navega por internet, su conciencia de responsabilidad y las medidas que deben tomar las administraciones públicas para mejorar la ciberseguridad.

- Módulo H: Comportamiento. Comprueba el comportamiento del usuario. Describe si el comportamiento del usuario es apropiado en relación con el uso de diferentes servicios de internet, como cumplir con las medidas de seguridad cuando se utiliza la banca en línea, descargas punto a punto (P2P) o redes sociales.

Las preguntas son de opción múltiple y su número de respuestas posibles varía de una pregunta a otra (entre 2 y 16). Por lo tanto, se necesita una conversión de este tipo nominal o categórico a un tipo numérico para calcular las estadísticas y poder utilizar técnicas de aprendizaje automático y visualización. La idea es escalar las variables entre 0 y 100. De esta manera, a cada usuario se le asigna un valor numérico en cada uno de los módulos de encuesta en función de su comportamiento en ese módulo (un valor alto si el comportamiento se considera positivo y uno bajo si se considera negativo). El siguiente paso es promediar todos los puntajes obtenidos para las preguntas del mismo módulo. Como resultado, se obtiene un puntaje promedio para cada uno de los 8 módulos. Esta recodificación en 8 variables reduce los costos computacionales y mejora la interpretabilidad.

Los datos presentados en este estudio se extrajeron de las siguientes fuentes:

- Datos declarados: obtenidos de las encuestas en línea dirigidas a hogares que definieron la muestra del estudio.
- Datos reales: obtenidos de un *software* de escaneo, que analiza los sistemas y la presencia de *malware* en ordenadores.

El *software* de escaneo utilizado fue iScan (luego renombrado como Pinkerton), desarrollado por la compañía de seguridad líder Hispasec. Este *software* se basa en el uso transparente y conjunto de 50 motores antivirus.

El *software* iScan se instaló en las computadoras de los usuarios y se utilizó para analizarlos, detectar *malware* que reside en los ordenadores y recopilar datos del sistema operativo. Además, analizó las herramientas de seguridad instaladas en los PCs y su estado de actualización. Los usuarios tenían una línea telefónica abierta para cualquier problema que pudieran encontrar. El sistema de recompensas para los usuarios consistía en puntos que podían canjearse como vales de regalo[1]. Con respecto a la privacidad y la ética de los datos, en España, los ciudadanos mayores de 15 años pueden participar en este tipo de estudio sin el consentimiento de sus padres. Al instalar el *software*, todos los usuarios están completamente informados sobre las políticas de privacidad con respecto a los datos recopilados.

4. RESULTADOS DE LAS ENCUESTAS DE CIBERSEGURIDAD

4.1. RESULTADOS GLOBALES

Esta sección presenta los resultados obtenidos sobre la encuesta de ciberseguridad tras aplicar los Mapas Auto-Organizados al conjunto de datos descrito en la sección anterior. Por lo tanto, esta sección detalla las conclusiones obtenidas para el estudio de la encuesta en su conjunto, es decir, teniendo en cuenta todos sus módulos.

[1]. Para más información sobre el sistema de recompensas ir a la web ASKGFK: https://www.askgfk.es/index.php?id=41

Cabe destacar dos cosas. Por un lado, este tipo de estudio únicamente es posible mediante el uso de una herramienta como el SOM, ya que las técnicas clásicas solamente pueden manejar visualizaciones precisas de conjuntos de datos completos cuando el número de características requeridas es igual o inferior a tres, tal y como se ha comentado en la introducción. Para representar un mayor número de características, solamente se pueden llevar a cabo proyecciones en tres dimensiones, estableciendo restricciones, como mantener fijo un cierto conjunto de variables y representar el resto. Por otro lado, hay que tener en cuenta que los resultados proporcionados en esta sección están basados en las respuestas de las encuestas proporcionadas por los usuarios. Por lo tanto, este estudio puede diferir ligeramente de la situación real, ya que los usuarios pueden ser desconocedores, o incluso mentir, en lo referente a ciertas preguntas o módulos. Por ello, se optó por realizar un segundo estudio incluyendo variables obtenidas por el *software* iScan (el cual mide situaciones reales) además de las de las encuestas. De este modo, se puede comparar las respuestas de los usuarios con la situación real en la que se encuentran sus equipos. Los resultados de dicho estudio se presentan en la siguiente sección.

Después de construir el conjunto de datos final, se procedió a entrenar dichos datos con los SOMs. Para el entrenamiento, se probaron diferentes opciones de los parámetros de ajuste del algoritmo del SOM, combinando todas las posibilidades (inicialización de los pesos, función de vecindad y tipo de entrenamiento). Además, la inicialización aleatoria se llevo a cabo 100 veces para cada combinación de parámetros. Por último, se seleccionó el SOM que mostró el mínimo error topográfico, que mide la preservación topología entre el espacio original y el espacio final. La Figura 4 muestra el mapa de componentes del SOM obtenido tras realizar el algoritmo de entrenamiento, explicado en la sección anterior. Se han marcado diferentes zonas de interés para ayudar al lector a la interpretación de los resultados.

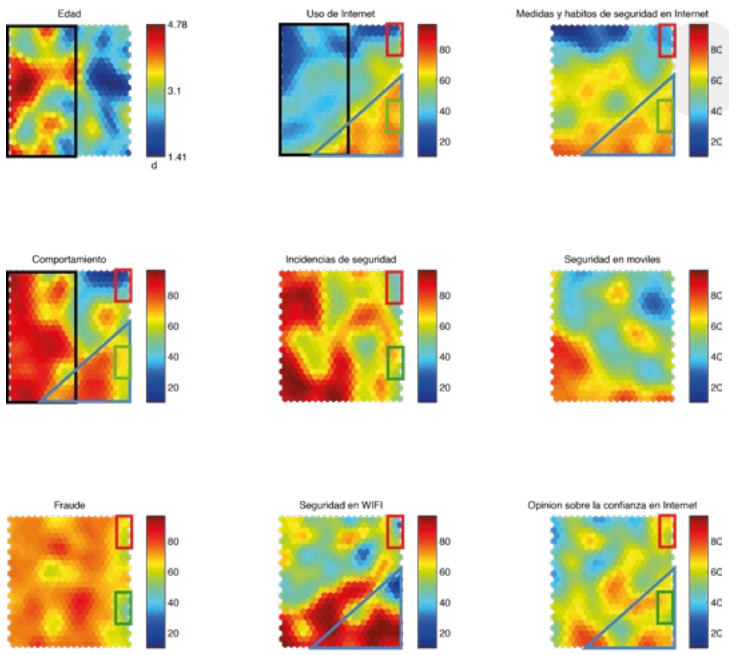


Figura 4. Mapa de componentes después del entrenamiento con los datos de la encuesta tras la 'fusión'.
Fuente: Elaboración propia.

Tras observar detenidamente dicha figura se pueden extraer las siguientes conclusiones:

- Centrando la atención en el área delimitada por el rectángulo negro, se puede observar que generalmente los usuarios de mayor edad (colores rojos) son los que menos utilizan los servicios de internet (colores azules).

- Siguiendo en esta zona, los usuarios de mayor edad (marcado por el rectángulo negro en la primera componente) son los que mejor comportamiento tienen (colores rojos en la cuarta componente). En cuanto a los jóvenes, existen tanto perfiles buenos como malos.

- Otra zona de interés es la delimitada por el triángulo azul. En esta zona se localizan los usuarios que más usan internet (segunda componente). Dichos usuarios son los que presentan mejores medidas de seguridad tanto en internet como en WIFI. Además, presentan un buen comportamiento y opinan que internet es de confianza.

- Otra zona de interés, de menor tamaño que el resto, pero no por ello menos importante, es la delimitada por el rectángulo verde. Esta zona ha sido marcada debido a que es la que presenta las peores puntuaciones en la componente Fraude (mayor nivel de fraude). Tal y como se observa, esta zona localiza a usuarios con alto uso de internet, con buenos hábitos de seguridad y buen comportamiento. A pesar de las malas puntuaciones en la componente Fraude, presentan valores buenos y medios en la componente 'Incidencias de seguridad'. A pesar de presentar fraude, dichos usuarios no tienen una opinión mala sobre la confianza en internet (última componente). Esto puede deberse a que el fraude realmente no está asociado con los hábitos de seguridad, sino que lo está con la confianza en internet; es decir, el hecho de que un usuario haya sido defraudado puede estar relacionado con que confía demasiado en internet independientemente de que utilice herramientas seguras para proteger su equipo.

- Otra zona de interés es la delimitada por el rectángulo rojo. Al igual que el caso anterior, se trata de una zona pequeña, pero de gran interés debido a que es la zona donde se encuentran las peores puntuaciones con respecto a incidencias de seguridad (mayor número de incidencias). Los usuarios localizados en esta zona presentan un perfil de bajo uso de internet, malas medidas de seguridad en internet y en Wi-Fi y mal comportamiento. Además, presentaron valores intermedios de fraude. A pesar de ello no tienen una muy mala opinión sobre la confianza en internet.

A parte del estudio del mapa de componentes obtenido tras el entrenamiento del SOM, se utilizó el mapa de ganadoras (explicado en la sección 2.2) para obtener mayor información. Tal y como se ha comentado anteriormente, un mapa de ganadoras convencional representa cada neurona mediante un hexágono en la cuadrícula del mapa. El área coloreada dentro de cada hexágono es proporcional al número de patrones de entrada que son más similares a esta neurona. Si además se colorea cada patrón de un color asociado a una clase, se obtiene una idea cuantitativa del número de vectores de entrada que pertenecen a cada neurona por cada clase. De esta manera, también es posible observar cómo se distribuyen los datos asociados a diferentes clases en el SOM. Por ejemplo, la Figura 5 (derecha) representa en diferentes colores la distribución en el SOM de los diferentes usuarios según el sistema operativo utilizado.

Por tanto, si existen tendencias claras (grupos aislados), podemos ver su caracterización, o comportamiento, observando los valores de cada variable en dichas áreas del mapa de componentes. La figura 5 se centra en sacar conclusiones sobre el sistema operativo utilizado en relación a la edad del usuario. Tal y como se observa, la gran mayoría de los usuarios más mayores suele utilizar Sistemas Operativos de la familia Windows (representado en color verde) y es reacio al uso de Unix/Linux (rojo) o de la familia Macintosh (azul). También resulta claro que el sistema operativo predominante en los usuarios encuestados pertenece a la familia Windows.

Además del estudio del sistema operativo en el SOM, se representó el mapa de ganadoras por colores de las variables Sexo, Ocupación, Estudios y Navegador. Estas figuras no se muestran en el presente estudio debido a que no condujeron a resultados concluyentes. Todas las clases estuvieron totalmente solapadas en todo el mapa, por lo que no existió un perfil concreto para dichas clases.

Después de presentar los resultados globales de las encuestas obtenidos por el SOM se ha observado que existen ciertas zonas de interés para estudiar en profundidad. Estas zonas, anteriormente mencionadas, se corresponden con las áreas delimitadas en los recuadros verde y rojo en la Figura 4. Tal y como se ha comentado, estas zonas presentan especial interés debido a que son las que menores puntuaciones presentaron en los bloques correspondientes a 'Fraude' e 'Incidencias de seguridad'. El procedimiento llevado a cabo para un estudio en mayor profundidad fue extraer los usuarios que se localizaban en cada una de las zonas concretas a estudiar y realizar nuevos entrenamientos con el algoritmo del SOM. La siguiente sección presenta los resultados obtenidos tras llevar a cabo dicho procedimiento.

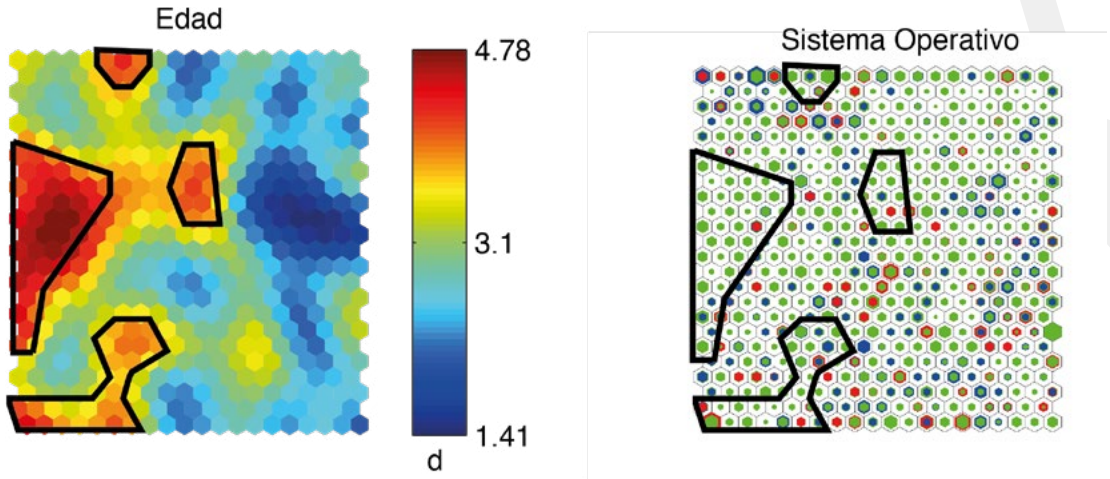


Figura 5. Relación de la edad del usuario con el Sistema Operativo que usa. A la izquierda, componente "Edad" extraída de la Figura 4. A la derecha, mapa de ganadoras con etiquetado por colores según sistema operativo. Windows (verde), Unix/Linux (rojo), Macinthosh (azul). Fuente: Elaboración propia.

4.2. RESULTADOS LOCALES: ZONA DE INTERÉS

Tal y como se ha mencionado, esta sección presenta los resultados de dos nuevos estudios realizados con los SOMs. Éstos se centran en un estudio "local", ya que se entrenan nuevos SOMs con subconjuntos de datos pertenecientes al conjunto global. Estos subconjuntos se centran básicamente en aquellos usuarios que, por un lado, presentaron las peores puntuaciones de fraude (mayor fraude de todas las encuestas) y, por otro lado, los que presentaron las peores puntuaciones en cuanto a incidencias de seguridad.

ANÁLISIS DE LA ZONA DE MÁXIMO FRAUDE.

Esta sección se centra concretamente en la zona del SOM que presentó mayores niveles de fraude (peores puntuaciones). La Figura 6 representa la localización de dicha área en el mapa de componentes global. La Figura 7 muestra el mapa de componentes del SOM obtenido tras realizar el algoritmo de entrenamiento sobre este subconjunto de datos. Tras observar detenidamente dicha figura se pueden extraer las siguientes conclusiones:

- Tras observar la zona delimitada por el recuadro negro se puede concluir que, en esta zona, de nuevo los usuarios de mayor edad son los que presentan un menor uso de los servicios de internet

- Además, se observa que la gente más mayor es también la que peores puntuaciones en incidencias de seguridad presentó. Una posible hipótesis es que esto se deba al desconocimiento, que generalmente es mayor en personas de mayor edad, de las nuevas tecnologías y de internet en particular.

- Un hecho curioso es la incongruencia observada en las componentes 'Incidencias de seguridad' y 'Medidas y hábitos de seguridad en internet'. Tal y como se observa en el área enmarcada en el recuadro azul, una mala puntuación (color azul) en los hábitos de seguridad conllevan las mejores puntuaciones en incidencias de seguridad (poco número de incidencias). Aunque cabe mencionar que las componentes 'Comportamiento' y 'Seguridad en Wi-Fi' obtienen buenas puntuaciones en esta zona. Lo mismo, pero de manera inversa, ocurre para la zona delimitada por el recuadro negro; una buena puntuación en seguridad acarrea una mala en infección. Este hecho llama la atención ya que cabe esperar que las incidencias de seguridad y las medidas de seguridad estén en cierta manera correlacionadas. Como se ha comentado anteriormente, este hecho puede deberse al desconocimiento de los usuarios sobre su nivel de infección o sobre sus medidas de seguridad, o simplemente se puede deber a que mienten.

Igual que en el caso del estudio global de las encuestas, se utilizó el mapa de ganadoras para obtener mayor información. La figura 8 representa en diferentes colores la distribución en el SOM de los diferentes usuarios según el sistema operativo utilizado. Tal y como se observó en el estudio global, la gran mayoría de los usuarios en la zona de mayor *Fraude* utilizaron sistemas operativos de la familia Windows (color verde), especialmente los más mayores.

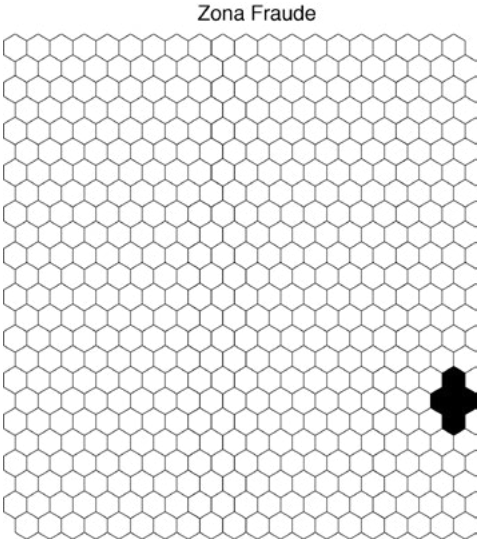


Figura 6. Localización de la zona a estudiar (Zona de máximo fraude) en el mapa de componentes global. Fuente: Elaboración propia.

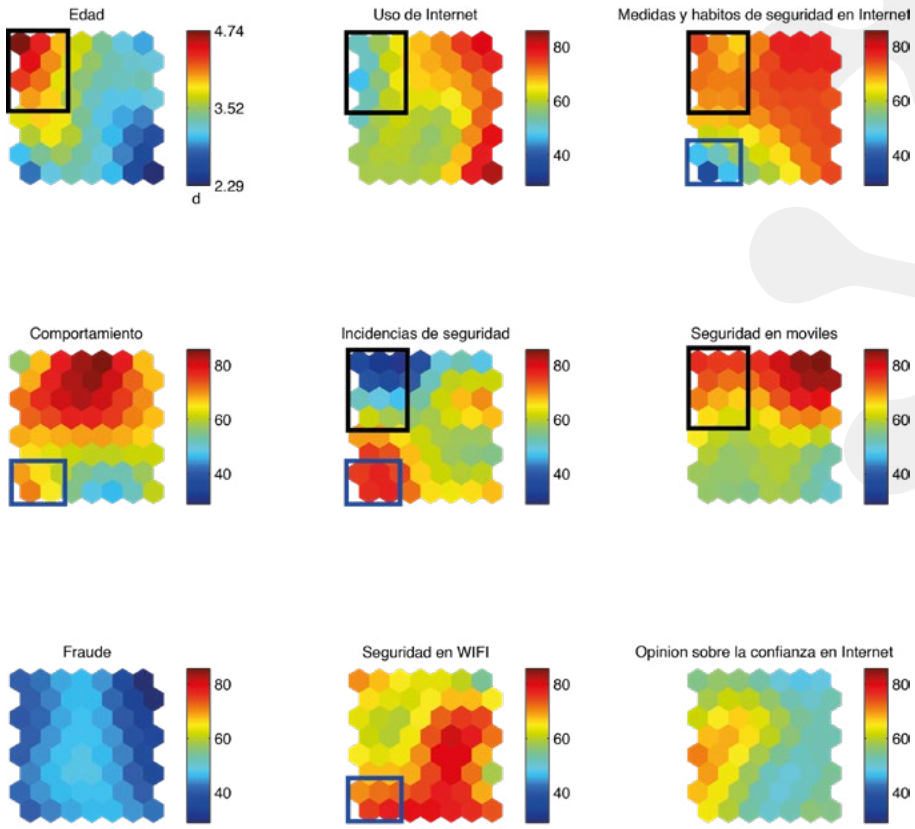


Figura 7. Mapa de componentes después del entrenamiento con el subconjunto de datos perteneciente a la zona de mayor fraude. Fuente: Elaboración propia.

Figura 8. Mapa de ganadoras con etiquetado por colores según el sistema operativo para el estudio local de la zona de mayor fraude. Windows (verde), Unix/Linux (rojo), Macintosh (azul). Fuente: Elaboración propia.

ANÁLISIS DE LA ZONA DE MÁXIMAS INCIDENCIAS DE SEGURIDAD.

Esta sección se centra concretamente en la zona del SOM que presentó peores puntuaciones en incidencias de seguridad. La figura 9 representa la localización de dicha área en el mapa de componentes global. La figura 10 muestra el mapa de componentes del SOM obtenido tras realizar el algoritmo de entrenamiento sobre este subconjunto de datos. Tras observar detenidamente dicha figura se pueden extraer las siguientes conclusiones:

- De nuevo es la gran mayoría de los usuarios jóvenes la que presenta un mayor uso de los servicios de internet (observar recuadro negro en las dos primeras componentes).
- Además, en esta zona a estudiar de nuevo los jóvenes son los que mejor comportamiento presentan (cuarta componente).
- Si se observa el área delimitada por el recuadro rojo, curiosamente se aprecia que los usuarios con peores puntuaciones en incidencias de seguridad (quinta componente) presentan alta puntuación en medidas y hábitos de seguridad (tercera componente) y viceversa. Esto puede ser a que realmente no sean conocedores de que sus equipos estén infectados y sus respuestas no reflejen la realidad.
- A pesar de que los usuarios localizados en esta zona bajo estudio presentan alta incidencia en seguridad, casi ninguno de ellos sufrió fraude (puntuaciones altas reflejadas por color rojo en todo el plano de componentes correspondiente a Fraude). Quizás por ello tienen una confianza relativamente alta sobre internet.

Igual que en los casos anteriores, se utilizó el mapa de ganadoras para obtener mayor información. La figura 11 representa en diferentes colores la distribución en el SOM de los diferentes usuarios según el sistema operativo utilizado. De nuevo se observa que la gran mayoría de los usuarios en la zona con mayores incidencias de seguridad utilizaron sistemas operativos de la familia Windows. Ninguno de ellos utilizó SO Unix/Linux.

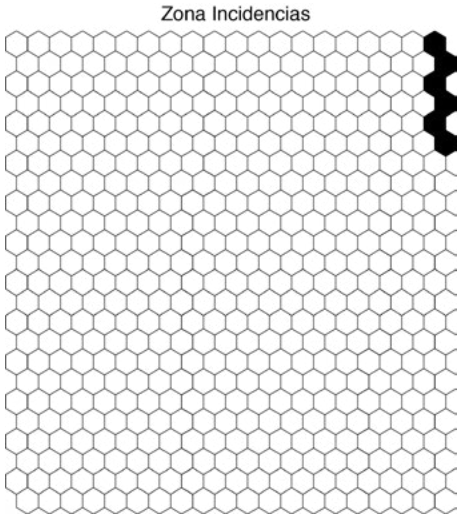


Figura 9. Localización de la zona a estudiar (Zona de máximas incidencias de seguridad) en el mapa de componentes global. Fuente: Elaboración propia.

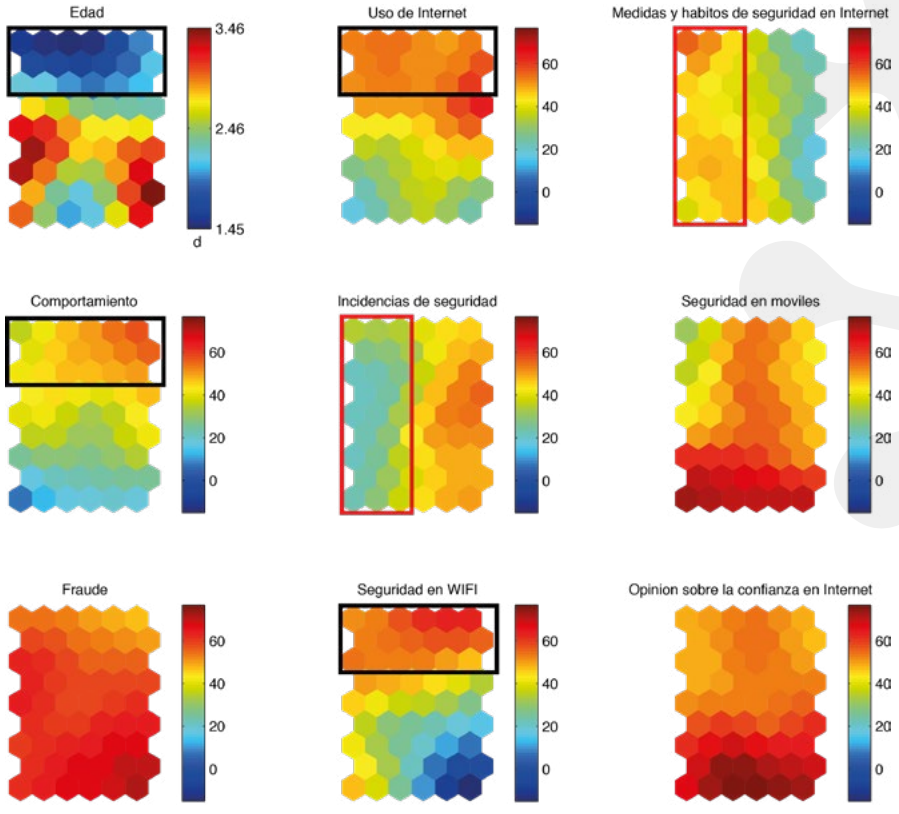


Figura 10. Mapa de componentes después del entrenamiento con el subconjunto de datos perteneciente a la zona de mayor número de incidencias. Fuente: Elaboración propia.

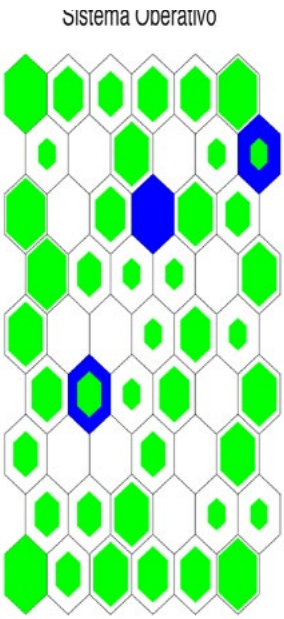


Figura 11. Mapa de ganadoras con etiquetado por colores según el sistema operativo para el estudio local de la zona de mayores incidencias de seguridad. Windows (verde), Unix/Linux (rojo), Macintosh (azul).
Fuente: Elaboración propia.

5. RESULTADOS DE LA ENCUESTA SOBRE CIBERSEGURIDAD JUNTO CON VARIABLES DEL *SOFTWARE* ISCAN

5.1. RESULTADOS GLOBALES

Esta sección presenta nuevos resultados obtenidos con el SOM tras incluir algunas variables del iScan en el entrenamiento. Concretamente, se utilizó la misma base de datos que en el caso anterior, pero añadiendo dos variables del iScan. Estas dos variables son las que resumen de manera general todas las variables medidas por el iScan. Éstas son 'Riesgo' y 'Total infecciones'. Tal y como se ha comentado anteriormente, los resultados proporcionados por la sección anterior están basados solamente en las respuestas de las encuestas proporcionadas por los usuarios. Por lo tanto, tal estudio puede diferir ligeramente de la situación real, ya que los usuarios pueden ser desconocedores, o incluso mentir, en lo referente a ciertas preguntas o módulos. Por ello, se optó por realizar un segundo estudio incluyendo variables obtenidas por el *software* iScan (el cual mide situaciones reales) además de las de las encuestas. Por tanto, se puede comparar las respuestas de los usuarios con la situación real en la que se encuentran sus equipos.

Cabe mencionar que para las variables referentes al iScan (*Riesgo* y *Total infecciones*) un valor alto hace referencia a un hecho negativo (alto riesgo o alto número de infecciones), no como ocurre con las variables procedentes de las encuestas donde se calcularon puntuaciones por bloque para las que un valor alto hace referencia a un buen comportamiento/medida y uno bajo a uno malo,

independientemente de que el bloque valore un aspecto negativo. Es decir, un valor de 100 en el módulo correspondiente a 'Fraude' conlleva a un hecho positivo en dicho módulo (no ha sufrido fraude) y no lo contrario. Además, cabe decir que en torno a un 31% de los usuarios que realizaron las encuestas no tienen mediciones del iScan. El aspecto positivo es que el SOM permite hacer un estudio de todos los pacientes, pero sin tener en cuenta las dos variables vacías (correspondientes al iScan) para estos usuarios.

Cabe mencionar también que la componente 'Total infecciones' se representa en escala logarítmica. En este caso los datos se mapearon de la siguiente forma: *log10(Totalinfecciones+1).* Esto se hizo así debido a que había algunos usuarios con valores muy extremos (llegando hasta 106), pero en su gran mayoría el resto de los usuarios presentaban valores mucho más bajos (de un orden inferior). Por lo tanto, la escala logarítmica permite observar todos los valores sin sesgar los colores del mapa en exceso. Observar que antes de aplicar el logaritmo en base 10 se suma 1 al número de infecciones. De este modo, se mantiene en la nueva recodificación un 0 si el número de infecciones es inexistente.

Tras entrenar el algoritmo del SOM con este nuevo conjunto de datos, se procede a visualizar el mapa de componentes obtenido (figura 12). De esta figura se extraen las siguientes conclusiones:

- Tal y como era de esperar, el número total de infecciones está correlacionado con el riesgo (comportamiento del usuario). Esto ocurre para las variables del iScan (medidas reales) y no tanto para las variables de las encuestas debido a que responden a medidas subjetivas. Se observa que la parte superior de ambas componentes se corresponde con un alto riesgo y un número alto de infecciones, mientras que la parte inferior localiza a usuarios con niveles muy bajos de infección y de riesgo.

- Se observa que no existen perfiles marcados en los usuarios que presentan riesgo e infecciones según iScan. Es decir, en el resto de variables (puntuación en cada módulo de la encuesta y edad) encontramos valores de todo tipo en el recuadro negro de la parte superior, desde mínimos a máximos. Es decir, encontramos todo tipo de puntuaciones (altas y bajas) en todos los módulos de manera que no se puede sacar una conclusión o perfilado concreto sobre estos usuarios (alto número de infecciones y riesgo alto según iScan). Por lo tanto, las respuestas de los usuarios en las encuestas no se corresponden exactamente con la realidad, ya que no hay una correlación entre las encuestas y el iScan (por ejemplo, una mala puntuación de comportamiento o medida de seguridad según la encuesta no siempre conlleva a riesgo o infección en iScan).

- Sin embargo, sí que se observa que en la zona de 'Riesgo' según iScan (parte superior del mapa) encontramos las peores puntuaciones de Fraude' (manchas verdes que representan valores intermedios).

- Se observa que los usuarios con peor puntuación en el bloque de comportamiento de la encuesta se encuentran en la zona de riesgo e infección según iScan (zona superior del mapa). En concreto se trata de la esquina superior izquierda de la componente 'Compor-

tamiento', donde se observan puntuaciones muy bajas en dicho bloque (color azul). Sin embargo, la zona de riesgo e infección según iScan (parte superior del mapa) también localiza a usuarios que, según ellos, tuvieron un comportamiento muy bueno (colores rojos). Además, se encuentran usuarios con mal comportamiento, según la encuesta, en la zona de "No riesgo" y "No infección" según iScan (zona inferior del mapa), en concreto en zona azulada localizada en la parte central-izquierda de la componente 'Comportamiento'.

- Si se observa las componentes correspondientes a 'Edad' y 'Total infecciones', se observa que los usuarios que presentan un mayor número de infecciones son los más jóvenes (zona delimitada por rectángulo rojo). Además, fueron los que presentaron peores puntuaciones en fraude (Fraude medio) tal y como explican las 3 "manchas" de color verde enmarcadas por el rectángulo rojo en la componente 'Fraude'.

Después de presentar los resultados globales de las encuestas junto con las variables del iScan obtenidos por el SOM, se ha observado que existe una zona de interés para estudiar en profundidad. Esta zona se corresponde con el área delimitada por el recuadro rojo en la Figura 12. Esta zona presenta especial interés debido a que es la que presentó el mayor número de infecciones y mayor número de fraude. El procedimiento llevado a cabo para un estudio en mayor profundidad fue extraer los usuarios que se localizaban en dicha zona y realizar nuevos entrenamientos con el algoritmo del SOM, al igual que en secciones anteriores. La siguiente sección presenta los resultados obtenidos tras llevar a cabo dicho procedimiento.

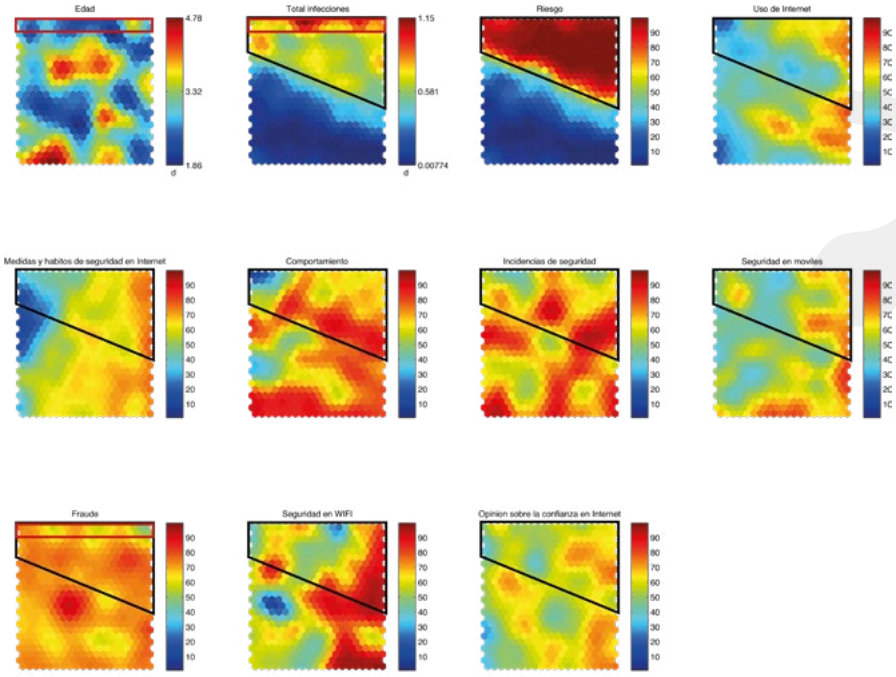


Figura 12. Mapa de componentes después del entrenamiento con los datos de las encuestas junto con las variables del iScan. Fuente: elaboración propia.

5.2. RESULTADOS LOCALES: ZONA DE INTERÉS

Tal y como se ha mencionado, esta sección presenta los resultados de un un estudio realizado usando los SOMs. Éste se centra en un estudio 'local', ya que se entrenan nuevos SOMs con un subconjunto de datos pertenecientes al conjunto global. Este subconjunto se centra básicamente en aquellos usuarios que presentaron los peores valores de fraude (mayor fraude de todas las encuestas) y mayor número de infecciones.

ANÁLISIS DE LA ZONA DE MÁXIMO NÚMERO DE INFECCIONES.

Esta sección se centra concretamente en la zona del SOM que presentó mayor número de infecciones. La Figura 13 representa la localización de dicha área en el mapa de componentes global. La Figura 14 muestra el mapa de componentes del SOM obtenido tras realizar el algoritmo de entrenamiento sobre este subconjunto de datos. Tras observar detenidamente dicha figura, se pueden extraer las siguientes conclusiones:

- Si se observa el área delimitada por el rectángulo negro, se comprueba que la gran mayoría de los usuarios que más infectados están según iScan (segunda componente) son los que presentan menores incidencias de seguridad según las encuestas (puntuaciones altas en la séptima componente). Este hecho carece de lógica, ya que cuanto mayor sea número de infecciones real medido por el *software* iScan, peor deberían ser las puntuaciones extraídas de las respuestas de las encuestas en el módulo incidencias de seguridad. Esto se debe a que los usuarios mienten en la encuesta, no son objetivos o ignoran el nivel de infección que presentan sus equipos.

- También se observa que dichos usuarios dijeron en las encuestas que tenían un buen comportamiento (valores altos en dicha componente), hecho que también carece de lógica debido al alto nivel de infección real. Sin embargo, la mayoría de ellos presenta una puntuación baja en el módulo 'Medidas y hábitos de seguridad en internet', lo cual coincide con el hecho de que el número total de infecciones sea alto.

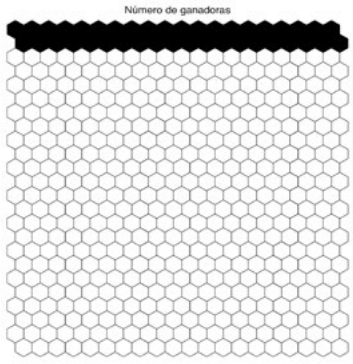


Figura 13. Localización de la zona a estudiar (Zona de máximo número de infecciones) en el mapa de componentes global. Fuente: Elaboración propia.

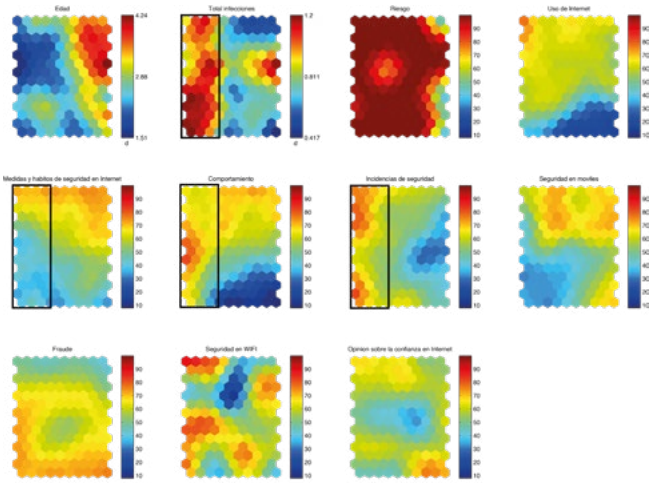


Figura 14. Mapa de componentes después del entrenamiento con el subconjunto de datos perteneciente a la zona de mayor número de infecciones según iScan. Fuente: Elaboración propia.

6. CONCLUSIONES

En esta sección se presentan las conclusiones más relevantes extraídas tanto del estudio de las encuestas de ciberseguridad, como del estudio realizado sobre dichas encuestas junto con las variables obtenidas con el *software* iScan. A continuación, se enumeran dichas conclusiones a modo de resumen:

ESTUDIO DE LAS ENCUESTAS DE CIBERSEGURIDAD:

- Generalmente los usuarios de mayor edad son los que tienen un menor uso de internet.
- Generalmente los usuarios más mayores son los que tienen un uso más responsable (mejor comportamiento) de internet. En los jóvenes se encuentran perfiles de todo tipo.
- Los usuarios que más usan internet son los que presentan mejores medidas de seguridad tanto en internet como en Wi-Fi. Además, presentan un buen comportamiento y opinan que internet es de confianza.
- Usuarios más defraudados presentan alto uso de internet, buenos hábitos de seguridad y buen comportamiento. Sin embargo, presentan valores buenos y medios en incidencias de seguridad. A pesar de ello no tienen una opinión mala sobre la confianza en internet. Esto puede ser a que el fraude realmente no está asociado con los hábitos de seguridad, sino que lo está con la confianza en internet.
- Sin embargo, los usuarios que mayores incidencias de seguridad tuvieron (puntuaciones bajas) presentan un perfil de bajo uso de internet, malas medidas de seguridad en internet y en Wi-Fi y mal comportamiento. Además, presentaron valores intermedios de fraude. A pesar de ello no tiene una muy mala opinión sobre la confianza en internet.

ESTUDIO DE LAS ENCUESTAS DE CIBERSEGURIDAD JUNTO CON VARIABLE ADQUIRIDAS CON EL ISCAN :

- Tal y como era de esperar, las infecciones están correlacionadas con el riesgo. Esto ocurre para las variables del iScan (medidas reales) y no tanto para las variables de las encuestas (medidas subjetivas).

- No existen perfiles marcados en los usuarios que presentan riesgo e infecciones según iScan; es decir, en el resto de variables encontramos valores de todo tipo, desde mínimos a máximos.

- Los usuarios que presentan un mayor número de infecciones reales son los más jóvenes. Además, fueron los que presentaron peores puntuaciones en fraude (Fraude medio).

- No existe una total correlación entre las encuestas y el iScan (por ejemplo, una mala puntuación de comportamiento o medida de seguridad según la encuesta no siempre conlleva a riesgo o infección en iScan).

- Tras estudiar la zona de interés (número alto de infecciones) se observó que la gran mayoría de los usuarios que más infectados están son los que presentan mejores puntuaciones en el bloque 'Incidencias de seguridad' de la encuesta. Además, dichos usuarios dijeron en las encuestas que tenían un buen comportamiento. Esto se puede deber a que mienten en la encuesta, no son objetivos o ignoran el nivel de infección que presentan sus equipos.

7. BIBLIOGRAFÍA

P, Friedman A. Cybersecurity and cyberwar: what everyone needs to know. Oxford University Press; 2014.

Kniwkes W, Prince D, Hutchison D, Disso JFP, Jones K. A survey of cyber security management in industrial control systems. Int J Crit Infraestructure Protect 2015; 9:52-80

Donaldson SE, Siegel S, Williams C, Aslam A. Enterprise cybersecurity how to build a successful cyberdefense program against advanced threats. Apress; 2015.

Gordon LA, Loeb MP, Lucyshyn W, Xhow L. The impact of information sharing on cybersecurity underinvestment: a real options perspective. J Account Public Policy 2015; 34(5):509-19

Bashir, M., Wee, C., Memon, N., & Guo, B. (2016). Profiling cybersecurity competition participants: self-ffi-cacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. Computers and Security 2017; 65:153:65

Davinson, N., Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. Computers in Human Behavoir, 26, 1739–1747.

Shillair, R., Cotten, S., Tsai, H., Alhabash, S., Rifon, N. (2015). Online safety begins with you and me: Convincing internet users to protect themselves. Computers in Human Behavior, 48, 199–207.

J., Urueña, A., Torres, A., Hidalgo, A. (2017). My computer is infected: the role of users sensation seeking and domain-specific risk perceptions and risk attitudes on computer harm. Journal of Risk Research, 20,

1466–1479.

CAPÍTULO VII

ISO 27001

FUNDAMENTOS

VI. ISO 27001. Fundamentos

Por Jorge Edo y Jorge Sánchez

* *Jorge Edo es director del Área de Tecnologías de la Información de Mobiliza Academy*

* *Jorge Sánchez es director de Mobiliza Academy*

1. INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN

Para entender bien el concepto de Seguridad de la Información, previamente necesitamos entender el concepto de información. Este concepto, se puede definir como un conjunto de datos procesados en poder de una empresa u organización, independientemente de la forma en que esta se guarde o transmita (escrita, oral, diagramas, digital, etc.).

Otro punto importante a tener en cuenta es que no hay que confundir los conceptos de Seguridad de la Información con el de Seguridad Informática. La Seguridad de la Información abarca muchas más áreas, mientras que la Seguridad Informática se encarga de la protección de las infraestructuras TIC que soportan el negocio. Por tanto, la Seguridad de la información abarca la Seguridad Informática.

Como se puede apreciar en la figura, hay otros aspectos que tenemos que tener en cuenta y que afectan a la Seguridad de la Información, como podemos apreciar en la figura siguiente.

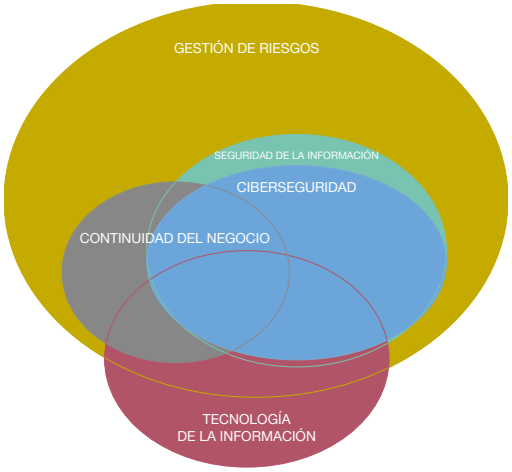


Figura 1. Áreas relacionadas con la Seguridad de la Información. Fuente: Inteco.

Analizando en detalle la figura, vemos que las áreas que abarcan la Seguridad de la Información y la Ciberseguridad son muy similares, y que la Ciberseguridad incluye a la Seguridad de la Información. Esto se debe a que, en el caso de la Seguridad de la Información, se incluye la información en papel, mientras que, en el caso de la Ciberseguridad, implica necesariamente una interconexión de Sistemas. Por otro lado, hay otras áreas como son: La Continuidad del Negocio, Las Tecnologías de la Información y la Gestión de los Riesgos que influyen de forma notable en la Seguridad de la Información.

Finalmente, una vez hechas las consideraciones anteriores, podemos definir la Seguridad de la Información como la protección de la confidencialidad, integridad y disponibilidad de la misma y de los activos de información de los que disponga la organización en función de la criticidad adecuada a su nivel de riesgo para alcanzar los objetivos de negocio de la entidad.

Estos tres parámetros básicos de la seguridad se definen como:

- **Confidencialidad:** Solo se permite a las personas debidamente autorizadas acceder a la información.
- **Integridad:** Mantenimiento de la exactitud y de forma completa de la información y sus sistemas de procesamiento.
- **Disponibilidad:** Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

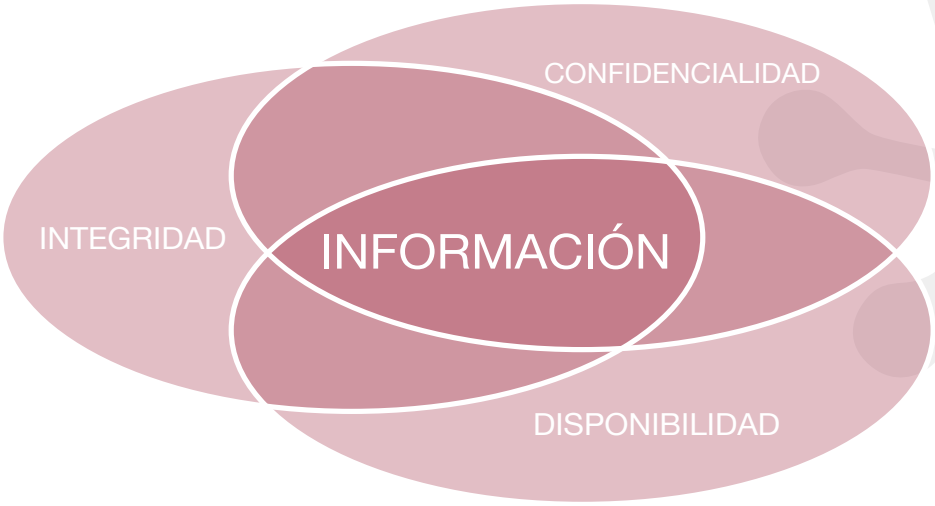


Figura 2. Parametros Básicos de la Seguridad de la Información. Fuente Inteco.

Viendo en detalle la definición anterior, hay que pensar que las organizaciones y sus Sistemas de Información y redes de comunicaciones, se enfrentan a diario a amenazas de seguridad procedentes de una amplia variedad de fuentes: ciberdelincuentes, espionaje empresarial, virus, troyanos,

vandalismo, incendios e inundaciones, entre otras, y que sólo una adecuada gestión de la Seguridad de la Información impedirá la perdida de uno de los principales activos de las empresas que es su información.

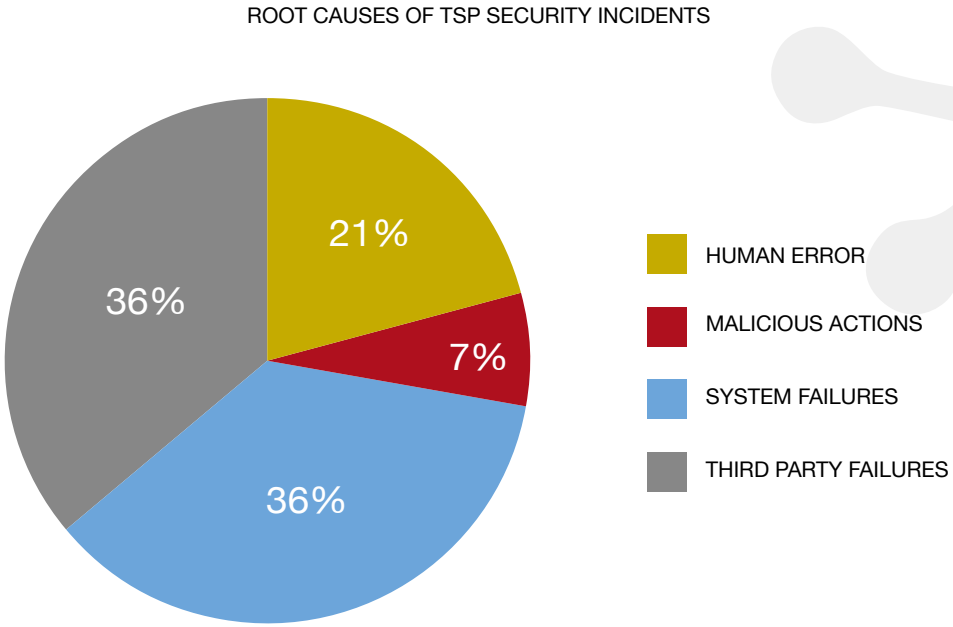
Dependiendo de las normativas, de los estándares utilizados o de las necesidades del negocio, en ocasiones además de la confidencialidad, la integridad y la disponibilidad, también son características de la información a tener en cuenta, tal y como recoge el Esquema Nacional de Seguridad (ENS), la Autenticidad y la Trazabilidad de la Información:

- **Autenticidad:** La información es lo que dice ser o el transmisor de la información es quién dice ser.
- **Trazabilidad:** Es la característica que aplicamos a la información que nos permite asegurar en todo momento quién hizo qué y cuándo lo hizo en relación con la información (ejemplo: modificación historias clínicas).

IMPORTANCIA DE LA SEGURIDAD

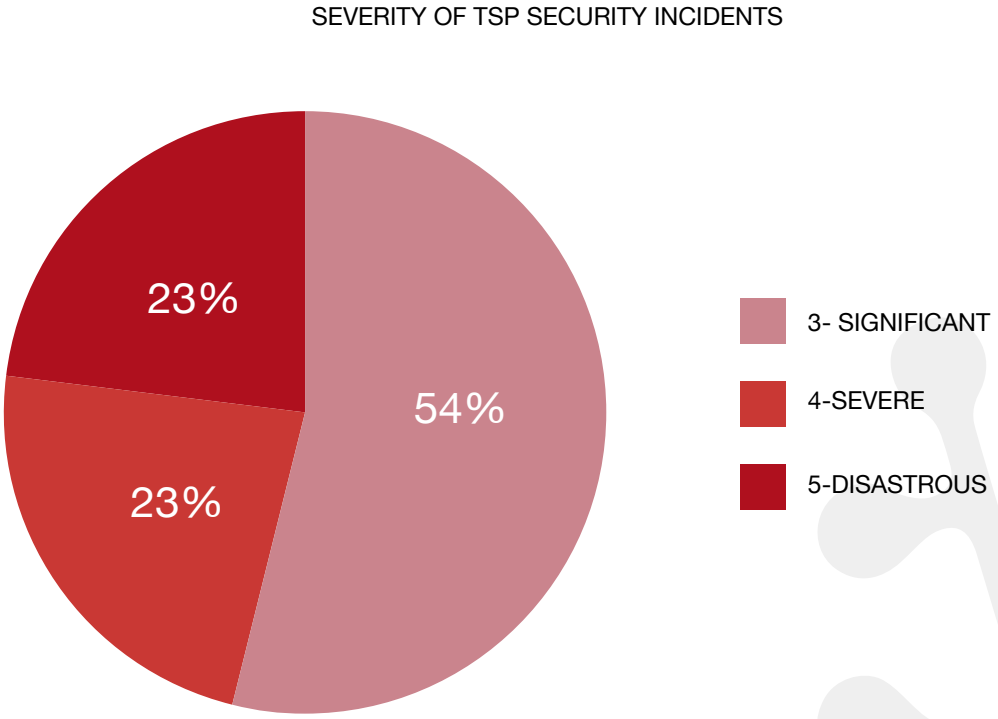
La Seguridad de la Información debe ser uno de los aspectos clave de la agenda de cualquier organización, independientemente de su sector económico o de su tamaño. La protección de la misma dependerá del tipo de empresa y la criticidad de los datos que maneja.

Los perjuicios que ocasionan los incidentes de seguridad son, cuando menos, incómodos y en muchos casos suponen pérdidas importantes para la compañía que los sufre. En el gráfico siguiente podemos ver las principales causas de incidentes de seguridad



Gráfica 1. Principales causas de incidentes. Fuente: Enisa. Annual Report Trust Services Security Incidents 2017. Octubre 2018. ISBN: 978-92-9204-258-5, DOI: 10.2824/835041

En el gráfico anterior podemos ver que un porcentaje muy importante de los incidentes de seguridad se deben a errores humanos (22%) y otro porcentaje considerable (un 36%) a errores de los sistemas. En cuanto a la gravedad de los incidentes, la figura siguiente nos da indicaciones en porcentaje de cómo afectan los incidentes a la empresas.



Gráfica 2. Importancia de los Incidentes de Seguridad. Fuente: Enisa. Annual Report Trust Services Security Incidents 2017. Octubre 2018. ISBN: 978-92-9204-258-5, DOI: 10.2824/835041

Los datos anteriores son datos a nivel europeo. En las dos gráficas siguientes se aprecia la evolución por años de los incidentes registrados en España a partir de los datos obtenidos por el Centro Criptológico Nacional Computer Emergency Response Team, también conocido por su sigla CCN–CERT
.

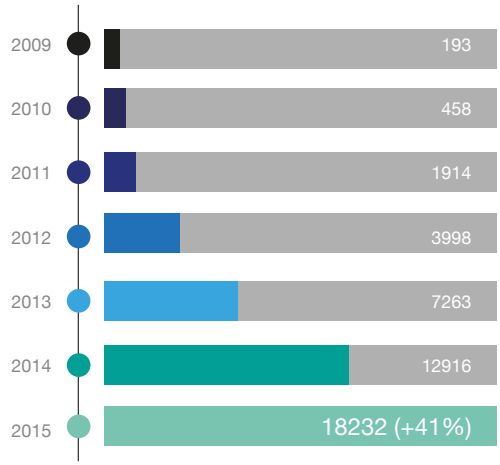


Figura 2. Incidentes registrados en el CC-Cert del 2009 al 2015. Fuente: CCN-Cert

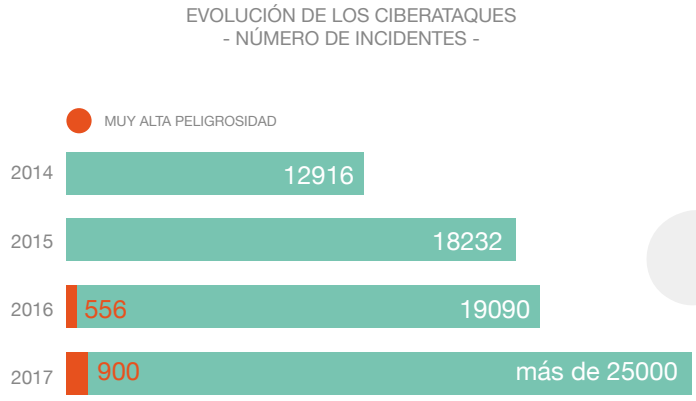


Figura 3. Evolución de los ciberataques en los últimos años. Fuente: CCN-Cert

2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Todos los incidentes que hemos visto anteriormente que amenazan la Seguridad de la Información requieren, cada día más, de sistemas de gestión acordes con el valor de la propia información para la organización y de los sistemas informáticos que los tratan. Un Sistema de Gestión de Seguridad de la Información o SGSI es aquella parte del sistema general de gestión de una organización que comprende:

- La política de seguridad de la información de la compañía
- La estructura organizativa
- los procedimientos

- los procesos y
- los recursos necesarios, para implantar la gestión de la seguridad de la información

Un SGSI podría considerarse como el sistema de calidad (de la ISO 9001) de la Seguridad de la Información. El propósito del SGSI no es garantizar la seguridad absoluta de la información de la compañía, sino garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible y adaptada a los cambios que se produzcan en la organización.

Los principales beneficios que aporta un proyecto de un SGSI son los siguientes:

- Mejora de la Seguridad de la Información
- Buen gobierno de la Seguridad de la Información
- Reducción de costes
- Conformidad y cumplimiento
- Marketing

3. INTRODUCCIÓN A LA NORMA ISO 27001

Como hemos visto anteriormente, un SGSI requiere un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para conseguir los objetivos de negocio. Se basa en una evaluación del riesgo y de los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar los riesgos de manera eficaz.

En la siguiente figura aparecen los conceptos básicos implicados en todo proyecto de implantación de un SGSI:

Confidencialidad
Propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.
(ISO 27000, 2.13)

Integridad
La propiedad de proteger la exactitud y completitud de los activos.
(ISO 27000, 2.36)

Disponibilidad
La propiedad de ser accesible y utilizable por una entidad autorizada.
(ISO 27000, 2.10)

No repudio
Capacidad para demostrar la existencia de un evento y sus entidades originarias.
(ISO 27000, 2.49)

Tabla 1. Conceptos básicos en un proyecto de implantación de un Sistema de Gestión de Seguridad de la Información (SGSI). Fuente: ISO/IEC 27001:2013

En la siguiente figura se recogen otros conceptos de interés:

Amenaza
Causa potencial de un incidente no deseado que puede acabar en daño para un sistema u organización.
(ISO 27000, 2.83)

Vulnerabilidad
Debilidad de un activo o control que puede ser explotada por una o más amenazas.
(ISO 27000, 2.89)

Impacto
Cambio adverso importante en el nivel de los objetivos de negocio logrados.
(ISO 27000, 3.1)

Riesgo
Potencialidad de que una amenaza explote una vulnerabilidad en un activo y cause daño a la organización.
(ISO 27000, 2.61)

Tabla 2. Otros conceptos de interés en un proyecto de implantación de un Sistema de Gestión de Seguridad de la Información (SGSI). Fuente: ISO/IEC 27001:2013

FAMILIA ISO 27000

La familia de normas ISO/IEC 27000 está compuesta por diversas normas. Destacamos las más importantes en la siguiente figura:

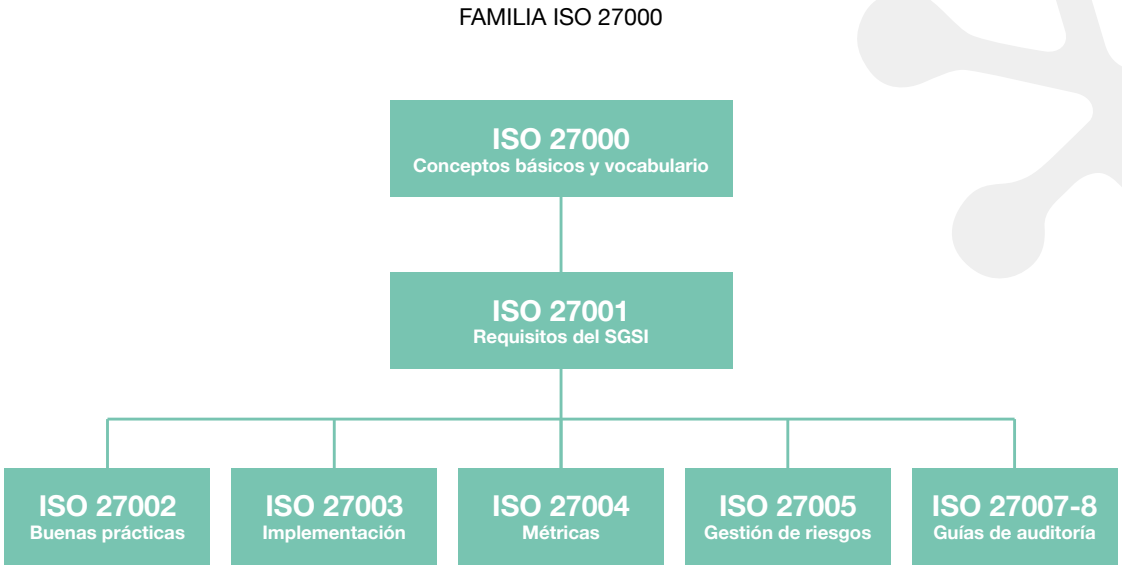


Figura 4. Familia de normas ISO / IEC 27000. Fuente: Elaboración propia.

OTROS MIEMBROS DE LA FAMILIA:

- ISO 27032. Ciberseguridad
- ISO 27034. Seguridad en el desarrollo de aplicaciones
- ISO 27035. Gestión de incidentes de seguridad. Esta norma también se puede utilizar de base para implementar los procedimientos de gestión de incidencias indicados en el Reglamento General de Protección de Datos (GDPR o RGPD)

ISO 27001

De todas las normas de la familia de la ISO 27000, la única que es certificable es la ISO 27001. La ISO/IEC 27001 es un estándar para la Seguridad de los Sistemas de Información publicado como estándar internacional en octubre de 2005 por la International Organization for Standarization (ISO). Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI). La versión actual se publicó en 2013. Los requisitos de esta norma aplican a todo tipo de organizaciones, independientemente de su tipo, tamaño o área de actividad.

La ISO/IEC 27001 es un estándar para la Seguridad de los Sistemas de Información que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

Como se puede apreciar en la figura siguiente, la norma consta de un cuerpo principal formado por las cláusulas que van de la 4 a la 10 y por un Anexo A formado por 114 controles agrupados en 35 objetivos de control o familias de categorización de los 114 controles.

DOCUMENTOS OBLIGATORIOS QUE EXIGE LA ISO 27001 PARA LA CERTIFICACIÓN.

A continuación, se indican la documentación necesaria que se exige en la norma para obtener la certificación:

- Alcance del SGSI (punto 4.3)
- Objetivos y política de seguridad de la información (puntos 5.2 y 6.2)
- Metodología de evaluación y tratamiento de riesgos (punto 6.1.2)

- Declaración de aplicabilidad (punto 6.1.3 d)
- Plan de tratamiento de riesgos (puntos 6.1.3 e y 6.2)
- Informe de evaluación de riesgos (punto 8.2)
- Definición de roles y responsabilidades de seguridad (puntos A.7.1.2 y A.13.2.4)
- Inventario de activos (punto A.8.1.1)
- Uso aceptable de los activos (punto A.8.1.3)
- Política de control de acceso (punto A.9.1.1)
- Procedimientos operativos para gestión de TI (punto A.12.1.1)
- Principios de ingeniería para sistema seguro (punto A.14.2.5)
- Política de seguridad para proveedores (punto A.15.1.1)
- Procedimiento para gestión de incidentes (punto A.16.1.5)
- Procedimientos para continuidad del negocio (punto A.17.1.2)
- Requisitos legales, normativos y contractuales (punto A.18.1.1)

REGISTROS OBLIGATORIOS QUE EXIGE LA ISO 27001 PARA LA CERTIFICACIÓN.

- Registros de capacitación, habilidades, experiencia y calificaciones (punto 7.2)
- Monitorización y resultados de medición (punto 9.1)
- Programa de auditoría interna (punto 9.2)
- Resultados de auditorias internas (punto 9.2)
- Resultados de la revisión por parte de la dirección (punto 9.3)
- Resultados de medidas correctivas (punto 10.1)
- Registros sobre actividades de los usuarios, excepciones y eventos de seguridad (puntos A.12.4.1 y A.12.4.3)

La ISO 27001 esta basada en un enfoque por procesos y en la mejora continua, por lo tanto, es perfectamente compatible e integrable con el resto de sistemas de gestión que ya existan en la organización. La norma asume que la organización identifica y administra cualquier tipo de acti-

vidad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas, puede ser considerada como un 'proceso'. A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos. Estos procesos se someten a revisiones para detectar fallos e identificar mejoras, por lo que se encuentran dentro de un proceso de mejora continua.

DEFINICIÓN DE PROCESO

Los procesos se pueden definir como un grupo lógico de tareas relacionadas entre sí para alcanzar un objetivo definido. Un proceso es una secuencia de actividades estructuradas y medidas diseñada para crear un producto o un servicio para un mercado específico o de un cliente en particular. Para que una organización funcione de manera eficaz, debe implementar y gestionar numerosos procesos ínter relacionados e interactivos.

A menudo el elemento de salida de un proceso constituye directamente el elemento de entrada del siguiente proceso. La identificación y gestión ordenada de los procesos dentro de una organización y, en especial, la interacción de estos procesos se denomina 'enfoque basado en procesos'.

La ISO 27001 podemos implementarla aplicando el Ciclo de Deming o de Espiral de Mejora Continua.

El ciclo de Deming (de Edwards Deming), también conocido como ciclo PDCA (del inglés Plan-Do-Check-Act) o PHVA (de la traducción al español como Planificar-Hacer-Verificar-Actuar) o Espiral de Mejora Continua, es el sistema más usado para implantar un sistema de mejora continua cuyo principal objetivo es la autoevaluación, destacando los puntos fuertes que hay que tratar de mantener y las áreas de mejora en las que se deberá actuar.

El ciclo PDCA de mejora continua lo componen cuatro etapas cíclicas de forma que una vez acabada la etapa final se debe volver a la primera y repetir el ciclo de nuevo. De esta forma, las actividades son revaluadas periódicamente para incorporar nuevas mejoras. A continuación, se describen en detalle las etapas que forman el Ciclo PDCA:

1. PLAN (PLANIFICAR):

En esta fase se trabaja en la identificación del problema o actividades susceptibles de mejora, se establecen los objetivos a alcanzar, se fijan los indicadores de control y se definen los métodos o herramientas para conseguir los objetivos establecidos.

Dos formas de identificar estas mejoras son, bien realizando grupos de trabajo, bien buscando nuevas tecnologías o herramientas que puedan aplicarse a los procesos actuales. Para detectar tecnologías o herramientas a veces es conveniente fijarse en otros sectores, pues aunque aporta una visión diferente, muchas de las soluciones pueden aplicarse a más de un sector.

2. DO (HACER O IMPLEMENTAR):

Llega el momento de llevar a cabo el plan de acción mediante la correcta realización de las tareas planificadas, la aplicación controlada del plan y la verificación y obtención del *feedback* necesario para el análisis que se realizará en la siguiente fase de verificación.

En numerosas ocasiones conviene realizar una prueba piloto para probar el funcionamiento antes de realizar los cambios a gran escala. La selección del piloto debe realizarse teniendo en cuenta que sea suficientemente representativo, pero sin que suponga un riesgo excesivo para la organización.

3. CHECK (COMPROBAR O VERIFICAR):

Una vez implantada la mejora, se comprueban los logros obtenidos en relación a las metas u objetivos que se marcaron en la primera fase del ciclo mediante herramientas de control (Diagrama de Pareto, listas de requisitos o *checklists*, indicadores de desempeño o *key performance indicators* –KPIs-, etc.)

4. ACT (ACTUAR):

Por último, tras comparar el resultado obtenido con el objetivo marcado inicialmente, es el momento de realizar acciones correctivas y preventivas que permitan mejorar los puntos o áreas de mejora, así como extender y aprovechar los aprendizajes y experiencias adquiridas a otros casos, y estandarizar y consolidar metodologías efectivas.

En el caso de que se haya realizado una prueba piloto, si los resultados son satisfactorios, se implantará la mejora de forma definitiva; y si no lo son, habrá que decidir si realizar cambios para ajustar los resultados sin desecharla. Una vez finalizado el paso 4, se debe volver al primer paso periódicamente para estudiar nuevas mejoras a implantar.

4. GESTIÓN DE LA SEGURIDAD DE LOS ACTIVOS. SEGURIDAD LÓGICA Y EN LOS PROCEDIMIENTOS. SEGURIDAD APLICADA A LAS TI Y A LA DOCUMENTACIÓN.

4.1. POLÍTICA DE SEGURIDAD

Con la definición de las políticas y estándares de seguridad informática se busca establecer dentro de la empresa una cultura de Seguridad Informática operando en una forma confiable. La Seguridad Informática es un proceso donde se deben evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades de la empresa en materia de seguridad.

Las normas y políticas sirven como referencia y en ningún momento pretenden ser normas absolutas -están sujetas a cambios realizables en cualquier momento-, siempre y cuando se tengan presentes los objetivos de seguridad de la información de la entidad donde aplican.

Así, las políticas de seguridad buscan ser la fuente de referencia y ser el medio de comunicación en el cual se establecen las reglas, normas, controles y procedimientos que regulen la forma en que la empresa proteja y maneje los riesgos de seguridad que ocurran en los diversos escenarios de riesgo que puedan originarse. La alta dirección de la empresa debe apoyar activamente la seguridad en el interior de la empresa, y para ello creará una Política de Seguridad de la Información, un conjunto de directrices que permite resguardar los activos de información.

¿Cómo debe ser una **Política de Seguridad de la Información** de una organización?

- Debe definir la postura de la dirección o la gerencia con respecto a la necesidad de proteger la información corporativa.
- Orientar a los usuarios con respecto al buen uso de los recursos de información.
- Definir la base para definir la estructura de seguridad de la organización.
- Ser un documento de apoyo a la gestión de TI y Seguridad Informática.
- Debe mantener el Principio de Neutralidad Tecnológica, es decir, ser general sin comprometerse con tecnologías especificas.
- Debe abarcar toda la organización.Debe ser de larga duración, manteniéndose sin grandes cambios en el tiempo.
- Debe ser clara y evitar confusiones o interpretaciones.
- Debe permitir poder clasificar la información en confidencial, uso interno y pública.
- Debe de identificar claramente funciones específicas de los empleados, como: responsable, encargado/a o usuario/a.

¿Qué elementos debe contener una **Política de Seguridad de la Información**?

- Políticas especificas
- Procedimientos
- Estándares o practicas
- Controles
- Estructura organizacional

A continuación, vamos a explicar en detalle cada uno de estos elementos.

1.- Políticas específicas

Definen en detalle los aspectos específicos que regulan el uso de los recursos tecnológicos y recursos de información. Suelen ser más susceptibles al cambio, a diferencia de la política general de la organización que suele permanecer más invariable con el tiempo.

Ejemplos de políticas específicas son, por ejemplo, el teletrabajo, el correo electrónico, el uso de internet, el uso de dispositivos móviles.

2.- Procedimientos

Los procedimientos:

- Definen los pasos para realizar una actividad especifica
- Evita que para realizar dicha actividad se aplique el criterio personal y cada uno lo realice de forma diferente

Ejemplos de procedimientos son el que rige las copias de seguridad, el procedimiento de actualización de antivirus o el procedimiento de actualización de servidores.

3.- Estándares

Es un documento establecido por consenso que sirve de patrón, modelo o guía, y que se usa de manera repetitiva. Los estándares de seguridad suelen ser actualizados periódicamente porque dependen directamente de la tecnología.

Ejemplos de estándares: ISO/IEC 27001:2017; ISO/IEC 22301:2015.

4.- Controles

El concepto de control dentro de una norma agrupa todo el conjunto de acciones, documentos, procedimientos y medidas técnicas adoptadas para garantizar que cada amenaza, identificada y valorada con un cierto riesgo, sea minimizada.

Ejemplos de controles: Anexo A de la ISO/IEC 27001.

La Política de Seguridad de la Información debe ser revisada y actualizada de forma conveniente de forma periódica, al menos una vez al año y previamente a la auditoría interna.

4.2. SEGURIDAD FÍSICA

Cuando establecemos la Seguridad Informática de una empresa, en ocasiones nos concentramos demasiado en las amenazas que pueden plantear los hackers, amenazas externas, y nos olvidamos de otro tipo de problemas que se pueden generar en nuestros datos si no tenemos cuidado. Nos referimos a los riesgos físicos, aquellos que son inherentes a cualquier tipo de organización y que pueden ser incluso más peligrosos que los de naturaleza digital.

¿Qué entendemos por Seguridad Física informática? La definición nos habla del proceso por el cual aplicamos una serie de barreras de tipo físico, así como unos procedimientos determinados, que nos permiten proteger nuestros recursos. Consiste en colocar contramedidas y sistemas de prevención para que la información confidencial que exista en nuestro negocio siempre esté a buen recaudo. Esta protección se instalará alrededor de los equipos informáticos para que el acceso a los mismos no sea sencillo y que todo dispositivo tecnológico en la empresa esté protegido. ¿Pero para qué elementos nocivos nos estamos protegiendo? ¿Qué es aquello que podemos considerar como una amenaza física para los sistemas informáticos de una empresa?

La Seguridad Física consiste en:

- **Disuasión:** establecimiento de límites físicos disuasorios ante posibles intentos de violación de la seguridad física. Por ejemplo, nos referimos a una valla de seguridad alrededor del recinto, un vigilante de seguridad o tornos de acceso al centro.
- **Denegación:** prohibición del acceso directo a elementos físicos.
- **Detección:** descubrimiento de las intrusiones.

El Centro de Proceso de Datos (CPD) es el lugar en el que se concentran todos los recursos necesarios para el procesamiento de información de una organización. Es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento informático y electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones, o bien como espacio de venta o alquiler. Por ejemplo, un banco puede tener un centro de procesamiento de datos con el propósito de almacenar todos los datos de sus clientes y las operaciones que estos realizan sobre sus cuentas. Prácticamente todas las compañías que son medianas o grandes tienen algún tipo de CPD, mientras que las más grandes llegan a tener varios.

Entre los factores más importantes que motivan la creación de un CPD, se puede destacar el garantizar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica.

El diseño de un centro de procesamiento de datos comienza por la elección de su ubicación geográfica y requiere un equilibrio entre diversos factores:

- **Coste económico**: coste del terreno, impuestos municipales, seguros, etc.
- **Infraestructuras disponibles** en las cercanías: energía eléctrica, carreteras, acometidas de electricidad, centralitas de telecomunicaciones, bomberos, etc.
- **Riesgo**: posibilidad de inundaciones, incendios, robos, terremotos, etc.

Una vez seleccionada la ubicación geográfica, es necesario encontrar unas dependencias adecuadas para su finalidad. Pueden ser de nueva construcción o un local ya existente que se comprará o alquilará. Algunos de los requisitos que deben cumplir estas dependencias son:

- Doble acometida eléctrica
- Muelle de carga y descarga
- Montacargas y puertas anchas
- Altura suficiente de las plantas
- Medidas de seguridad en caso de incendio o inundación: drenajes, extintores, vías de evacuación, puertas ignífugas, etc.
- Aire acondicionado, teniendo en cuenta que se usará para la refrigeración de equipamiento informáticoAlmacenes

Los CPDs exigen condiciones específicas de temperatura, que debería mantenerse entre 18 y 27 grados.

Deben contar también con sistemas de protección contra incendios, así como implementar programas de prevención de incendios. Normalmente se utilizan los siguientes sistemas divididos en dos grandes grupos: sistemas de detección y sistemas de extinción.

Sistema de detección

- Detector de calor (umbral de temperatura)
- Detector de llama (detector de energía infrarroja)
- Detector de partículas de combustión o humo

Sistema de extinción

- Extintores
- Sistemas de aspersión de agua
- Sistema de descarga de gas (CO2, Halón, …)

Recomendaciones en relación con el CPD

• UBICACIÓN

Un CPD no debería estar situado

- En la última planta (incendios)
- En el sótano (inundaciones)
- Cerca de áreas públicas del edificio (seguridad)

• ACCESO

Los principales sistemas de acceso a CPD son:

- Llave, tarjeta inteligente (rfid)
- Código de seguridad
- Sistemas biométricos
- Vigilante de seguridad
- Puertas de seguridad

• ELEMENTOS A TENER EN CUENTA

- Cámaras de vigilancia circuito cerrado en el CPD
- Alarmas: Sensores de movimiento, peso, etc.
- Auditoría de accesos al CPD
- Las puertas de seguridad
    - Sistema de auto-cierre y no permitir que se queden abiertas

- Alarmas automáticas en caso de ser forzadas o permanecer abiertas más de un cierto periodo
- Sistema de doble puerta (**mantrap**).
    - Después del cierre de la primera puerta, identifica y autentica un individuo antes de abrir la segunda puerta
    - Evita el **piggybacking.** Un individuo sin acceso aprovecha pasando detrás antes del cierre de puerta de un individuo autorizado

4.3. SEGURIDAD LÓGICA Y EN LOS PROCEDIMIENTOS

La Seguridad Lógica se refiere a la seguridad en el uso de *software* y los sistemas, en la protección de los datos, procesos y programas, así como en el acceso ordenado y autorizado de los usuarios a la información. Involucra a todas aquellas medidas establecidas por la administración -usuarios y administradores de recursos de tecnología de información- para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información. SLa laél.

La Seguridad Lógica involucra a todas aquellas medidas que minimizan los riesgos de seguridad asociados con las operaciones cotidianas de los usuarios de la empresa llevadas a cabo utilizando TIC

El activo más importante de un sistema informático es la información y, por tanto, la Seguridad Lógica se plantea como uno de los objetivos más importantes.

Trata de conseguir los siguientes objetivos:

- Restringir el acceso a los programas y archivos
- Asegurar que los usuarios puedan trabajar sin supervisión y no puedan modificar los programas ni los archivos que no correspondan
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto
- Verificar que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y que la información recibida sea la misma que la transmitida
- Disponer de rutas alternativas de emergencia para la transmisión de información

La Seguridad Lógica se encarga de los controles de acceso que están diseñados para salvaguardar la integridad de la información almacenada de un ordenador, así como de controlar el mal uso de la información. Asimismo, se encarga de controlar y salvaguardar la información generada por los sistemas, por el *software* de desarrollo y por los programas en aplicación.

Deberá identificar individualmente a cada usuario y sus actividades en el sistema, y restringir el acceso a datos, a los programas de uso general, de uso especifico, de las redes y terminales. La falta de Seguridad Lógica o su violación puede traer las siguientes consecuencias a la organización:

- Alteración de la integridad de los datos
- Copias de programas y /o información Código oculto en un programa
- Aparición de virus

5. ISO 27001 Y RECUPERACIÓN DE DESASTRES Y CONTINUIDAD DEL NEGOCIO.

5.1. INTRODUCCIÓN

Antes de meternos en detalle acerca de cómo implementar un Plan de Continuidad de Negocio, lo primero que deberiamos preguntarnos es cuál es la necesidad del mismo. Los acontecimientos que conocemos diariamente por los medios de comunicación prueban que las organizaciones no pueden estar preparadas para evitar cada uno de los eventos adversos que pueden sucederles y que pueden impactar en sus actividades de negocio.

ALGUNOS EJEMPLOS DE DESASTRES

Existen multitud de ejemplos que podemos enumerar acerca de situaciones de desastre, que daría para escribir varios libros. Pero podemos indicar los siguientes como una muestra de desastres producidos tanto a nivel nacional como internacional:

A NIVEL INTERNACIONAL

- El atentado terrorista de las Torres Gemelas el 11 de septiembre de 2001
- La llegada de Anonymous en 2003. Sus ataques son famosos porque afectan a importantes organizaciones del mundo entero, como el Vaticano, el FBI, la CIA, la OTAN y más de 650 sitios web de Israel de forma simultánea, entre otros. Tampoco se libra la Policía Nacional española.

- Robo de millones de cuentas de tarjetas de crédito en junio de 2005. Un ataque de CSS a uno de los principales procesadores de pagos, CardSystems, puso al descubierto más de 40 millones de tarjetas de crédito. Hackers hasta el momento desconocidos atacaron la base de datos con un troyano SQL encargado de insertar un código que repetía el ataque cada cuatro días y guardaba información en un archivo zip que era enviado a los atacantes. Obtenían información de nombres de acceso, números de cuentas y códigos de verificación.

- Noviembre de 2008: Conficker el gusano. El gusano Conficker, por su peligro y complejidad, se catalogó como una amenaza de nivel militar. Cuando un equipo es infectado, puede ser controlado a través de una red masiva que puede atacar a cualquiera. En sólo unas semanas infectó a más de 9 millones de equipos en todo el mundo, desde sistemas pertenecientes a la Armada Francesa hasta hospitales británicos.

- Uno de los ataques DDoS más importantes de la historia ocurrió en julio de 2009. Durante tres días importantes medios e industrias de todo el mundo fueron víctimas de uno de los principales y más peligrosos ataques de denegacion de servicio (DdoS) de toda la historia. La infección se dio a través de una red de bots enviada desde Corea del Norte a través del gusano Mydoomdonde.

- Stuxnet, un *malware* sofisticado, llegó en junio de 2010. Declarado como el *malware* más innovador de nuestros días, actúa como un espía que roba información, pero que además reprograma sistemas con el fin de ocultar los cambios realizados. Stuxnet fue controlado casi un año después, aunque una de sus novedades más sorprendentes han sido las variantes y conexiones que se han encontrado años después: Duqu en septiembre de 2011 y Flame en mayo de 2012.

- Robo de información de la marca de seguridad digital VeriSign en 2010. Fue atacada por cibercriminales a lo largo de todo un año, teniendo acceso a sistemas e información privilegiada de la compañía.

- Abril 2011: Millones de cuentas hackeadas de PlayStation Network. Es considerada como la peor violación de datos a una comunidad de juegos de todos los tiempos. Se obtuvieron datos de cuentas de usuarios de PlayStation, entre ellos, nombres, contraseñas, correos electrónicos, direcciones e historial de compras. En concreto, se vieron afectadas más de 77 millones de cuentas, de las cuales cerca de 12 millones también contenían el número de tarjetas de crédito.

- Troyano invade Macs en septiembre de 2011. El Troyano Flashback acabó con la invulnerabilidad de los equipos Apple y se presentaba como un PDF o un instalador de Flash Player que, al descargar y abrir, instalaba un acceso de BackDoor o puerta trasera. Una vez dentro, el troyano envía información sobre el equipo infectado a un servidor central.

- Ataque a favor de Megaupload en enero de 2012. Tras el cierre del sitio web de intercambio de archivos más importante del mundo, Anonymous realizó un hackeo masivo a 18 páginas web tales como la Casa Blanca, el Departamento de Justicia, la Oficina General del Copyright, Universal Music y diferentes sitios de la industria musical y cinematográfica.

- En diciembre 2013 las tarjetas de crédito de los clientes de Target salen a la luz. La cadena de tiendas Target en USA sufre un ciberdelito en todos los terminales de sus casi 2000 tiendas. Durante 15 días los ciberdelincuentes consiguen obtener 70 millones de tarjetas de crédito de los clientes de la cadena.

- 27 de mayo del 2017, caída del sistema informático de British Airways. Todas las operaciones de vuelo de la aerolínea británica desde los aeropuertos londinenses de Gatwick y Heathrow fueron suspendidas, lo que provocó la cancelación de más de 1.000 vuelos en todo el mundo y dejó a más de 75.000 pasajeros tirados en 170 aeropuertos de 70 países diferentes. El desastre se originó por una caída en la alimentación del CPD, problemas con el SAI y grupo electrógeno y una mal operativa en el procedimiento de contingencia

En España han tenido lugar los siguientes casos:

- 12 de mayo 2017. Una decena de grandes empresas españolas de servicios sufrieron ese viernes un ciberataque masivo a través de un virus malicioso, de tipo *ransomware*, que bloqueó los equipos y donde se solicitó un rescate para desbloquearlos. La compañía más afectada fue Telefónica de España.

- Julio de 2007. El fallo de la red eléctrica de Barcelona impactó en servicios críticos como sanidad y transporte.

- Febrero de 2005. El incendio del edificio Windsor en Madrid. El incendio provocó la pérdida de los soportes documentales de una auditoría realizada por Deloitte al Grupo FG, que habían sido solicitados por la Fiscalía Anticorrupción un día antes del siniestro. El bufete Garrigues también tenía presencia en el Windsor así como El Corte Inglés y tiendas y restaurantes en la planta baja. No fueron los únicos damnificados. En los alrededores, más de 140 negocios acabaron asociándose para reclamar las pérdidas que les ocasionó la catástrofe, que cifraron en 1,2 millones de euros.

Cada año son millones las organizaciones que padecen inundaciones, incendios, ataques terroristas, actos vandálicos y otras amenazas. Las compañías que logran superar estos desastres son las más previsoras, las que están preparadas para enfrentarse a lo peor, las que estiman los posibles daños que pueden sufrir y ponen en marcha las medidas necesarias para protegerse.

BENEFICIOS QUE PUEDE APORTAR UN PLAN DE CONTINUIDAD DE NEGOCIO

Además de prevenir o minimizar las pérdidas para el negocio que un desastre puede causar, el objetivo principal de cualquier programa orientado a gestionar la continuidad de negocio de una organización es garantizar que ésta dispone de una respuesta planificada ante cualquier trastorno importante que puede poner en peligro su supervivencia. Esta afirmación de por sí constituye un argumento irrefutable que explica la necesidad de instaurar en todas las compañías tales estrategias, independientemente de su tamaño y/o sector de actividad.

De todas ellas, vamos a detenernos con un poco más de detalle en las siguientes:

- **Ventaja competitiva frente a otras organizaciones**: el hecho de mostrar que se toman medidas para garantizar la continuidad de negocio mejora la imagen pública de la organización y revaloriza la confianza frente a accionistas, inversores, clientes y proveedores. Por otra parte, el retorno de la inversión (ROI) en aspectos de continuidad es más perceptible en términos de reputación e imagen pública.

- **Previsible y eficaz respuesta a las crisis**: a través de la gestión de la continuidad, una organización es capaz de abordar la gestión proactiva de amenazas y riesgos que pueden impactar en sus operaciones.

- **Reducción de costes y prevenir o minimizar las pérdidas de la organización en caso de desastre**: es capaz de identificar de forma proactiva los posibles impactos e inconvenientes que una interrupción de sus actividades de negocio puede provocar.

- **Cumplimiento de las normativas**: implantar con éxito una ISO 22301 provoca un menor riesgo de sufrir sanciones económicas al adaptarse a requerimientos normativos. En el caso de algunos sectores de actividad (infraestructuras críticas, bancario, aseguradoras) la adopción de planes de continuidad de negocio es un requerimiento regulatorio que debe ser satisfecho. El cumplimiento de tal requerimiento evita el riesgo de sufrir sanciones económicas.

5.2. ISO 27001 Y NORMA ISO 22301

La norma ISO que establece las indicaciones de cómo realizar un Plan de Continuidad de Negocio es la ISO 22301. Proporciona todos los requisitos necesarios para diseñar, implantar, mejorar y certificar un Sistema de Gestión de Continuidad del Negocio.

La norma ISO 22301:2012 es la primera norma internacional para la gestión de la continuidad de negocio y se ha desarrollado para ayudar a las empresas a minimizar el riesgo del tipo de interrupciones.

Esta norma especifica los requisitos necesarios para planificar, establecer, implantar, operar, monitorear, revisar, mantener y mejorar de forma continua el Sistema de Gestión para responder y recuperarse pronto de las interrupciones, en el momento en el que sucedan. Los requisitos que se especifican en la norma son genéricos y son aplicables a todas las empresas, no importa su tamaño, naturaleza o tipo. El grado de aplicación de los requisitos que vienen definidos en la norma depende del tipo de procesos y de la complejidad de la empresa.

La ISO 22301:2012 define los siguientes conceptos:

Continuidad del negocio: capacidad de la organización para continuar la entrega de productos o servicios a los niveles predefinidos tras un incidente perjudicial.

Gestión de continuidad del negocio: proceso de gestión holístico que identifica amenazas potenciales para la organización, así como el impacto en las operaciones del negocio que dichas amenazas, en caso de materializarse, puedan causar, y que proporciona un marco para aumentar la capacidad de resistencia o resiliencia de la organización para dar una respuesta eficaz que salvaguarde los intereses de sus principales partes interesadas, la reputación, la marca y las actividades de creación de valor.

Sistema de Gestión de la Continuidad del Negocio (SGCN): parte del sistema de gestión global que establece, implementa, opera, supervisa, revisa, mantiene y mejora la continuidad del negocio. El sistema de gestión incluye la estructura organizativa, políticas, actividades de planificación, responsabilidades, procedimientos, procesos y recursos.

Plan de Continuidad del Negocio: procedimientos documentados que orientan a las organizaciones a responder, recuperar, reanudar, y restaurar a un nivel pre-definido de funcionamiento tras una interrupción. Por lo general, esto incluye los recursos, los servicios y las actividades necesarias para asegurar la continuidad de las funciones críticas de la empresa.

Programa de Continuidad del Negocio: proceso continuo de gestión y dirección apoyado por la alta gerencia y con recursos adecuados para implementar y mantener la gestión de la continuidad del negocio.

Business Impact Analysis (BIA): proceso de análisis de funciones organizacionales y el efecto de una interrupción en ellas.

Conformidad: cumplimiento de un requerimiento.

Mejora continua: actividad para mejora del desempeño.

Corrección: acción para eliminar una no conformidad detectada.

Acción correctiva: acción para eliminar la causa de una no conformidad u otra situación no deseada y prevenir su recurrencia.

Otras definiciones de interés que incluye son:

EVENTO (ISO 22301, 3.17)	• Ocurrencia de un conjunto particular de circunstancias.
INTERRUPCIÓN (ISO 22399, 3.4)	• Evento que pudiera constituir o pudiera redundar en una interrupción del negocio, en una pérdida, emergencia o crisis.
INCIDENTE (ISO 22301, 3.19)	• Incidente, ya sea previsto (p.ej., un huracán) o imprevisto (por naturales, que requieren de atención urgente y de medidas para proteger la vida, los bienes o el medio ambiente.
CRISIS (USO 22399, 3.3)	• Cualquier incidente(s), causado por los humanos o causas naturales, que requieren de atención urgente y de medidas para proteger la vida, los bienes o el medio ambiente.
DESASTRE (ISO 22300, 2)	• Situación en la que se han producido amplias pérdidas humanas, materiales, económicas o ambientales que superaron la capacidad de la organización, la comunidad y la sociedad afectadas para responder y recuperarse utilizando sus propios recursos.
EMERGENCIA (ISO 22399, 3.6)	• Suceso o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.

Tabla 3. Definición de interés en las normas ISO. Fuente: ISO/IEC 22.301:2012

5.3. PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (SGCN):

Como hemos visto en el punto anterior, la norma 22301 es la normativa ISO que define las reglas para implementar y gestionar un SGCN. Sus características son las siguientes.

- Los requisitos (cláusulas) son escritos utilizando el verbo “deberán” en imperativo
- Integra el modelo PDCA (Plan, Do, Check, Act), al igual que ocurre con la ISO 27001 y el GDPR
- Es auditable
- La organización puede ser certificada en esta norma

UN SISTEMA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (SGCN)

a igual que cualquier otro sistema de gestión, tiene los siguientes componentes fundamentales:

1. Una política
2. Personas con responsabilidades definidas
3. Procesos de gestión asociados con:
    - Política
    - Planificación
    - Implementación y operación
    - Evaluación del rendimiento

- Revisión por la Dirección
- Mejora

4. Documentación que provea pruebas auditables

5. Cualquier proceso de gestión de la continuidad del negocio pertinente a la organización

Un SGCN consiste en la preparación proactiva de la organización frente a contingencias de todo tipo que puedan suponer una interrupción de la actividad de una empresa, suponiendo perjuicios de diferente gravedad según la importancia del ámbito donde se ha producido el paro y el tiempo de inactividad.

Puede considerarse, por lo tanto, como la capacidad estratégica y táctica de una organización para planificar y responder ante incidentes o interrupciones de negocio, con el fin de continuar las operaciones a un nivel aceptable de servicio, que debe definirse previamente. En los casos más graves la interrupción de la continuidad del negocio puede suponer la propia desaparición de la empresa, al producirse daños irreparables, pérdidas económicas inasumibles o la imposibilidad de hacer frente a pedidos o compromisos claves con los clientes.

MEJORA CONTINUA PDCA

La norma ISO 22301 adopta al igual que ocurre con la ISO 27001 y el RGPD el modelo de proceso "Planificar-Hacer-Verificar-Actuar" (PDCA), llamado también ciclo de Deming, que se aplica a la estructura de todos los procesos en un sistema de gestión.

La figura siguiente muestra cómo un sistema de gestión utiliza como entrada los requisitos y las expectativas de las partes interesadas, y cómo se producen, con las acciones y procesos necesarios, los resultados de Continuidad del Negocio que cumplan con los requisitos y expectativas.

Planificar (establecer el sistema de gestión): establecer la política, los objetivos, procesos y procedimientos relacionados con la gestión de riesgos y la mejora de la Continuidad del Negocio para ofrecer resultados en línea con las políticas y objetivos globales de la organización.

Hacer (implementar y operar el sistema de gestión):implementar y operar la política, controles, procesos y procedimientos del sistema de gestión.

Verificar (monitorizar y revisar el sistema de gestión): evaluar y, si procede, medir las actuaciones del proceso frente a la política, los objetivos y la experiencia práctica e informar los resultados a la gerencia para su revisión.

Actuar (mantener y mejorar el sistema de gestión): llevar a cabo las acciones correctivas y preventivas sobre la base de los resultados de la auditoría interna y revisión por la dirección, u otra información relevante para la mejora continua de dicho sistema.

5.4. ESTRUCTURA DE LA NORMA ISO 22301

Viene resumida en la tabla siguiente:

Sección 1	Ámbito de aplicación
Sección 2	Referencias normativas
Sección 3	Términos y definiciones
Sección 4	Contexto de la organización
Sección 5	Liderazgo
Sección 6	Planificación
Sección 7	Apoyo
Sección 8	Funcionamiento
Sección 9	Evaluación del desempeño
Sección 10	Mejora

Tabla 4. Estructura de la norma ISO 22301. Fuente: Elaboración propia.

DESARROLLO DE UN PLAN DE CONTINGENCIA

El plan de contingencia se enmarca dentro del plan de riesgo de la organización y, siguiendo los requisitos de la norma ISO 22301, se implementa como hemos visto anteriormente mediante un ciclo de mejora continua de Deming basado en un modelo PDCA.

Los principales elementos que debe tener un plan de contingencia son los siguientes:

1.- Definición de las situaciones críticas

Es importante definir los activos críticos y la relación de procesos de negocio que afecten a esos activos previamente identificados.

2.- Asignación de responsabilidades

Se deben crear grupos humanos configurados por personal competente como el comité de emergencia, el cual se encargará de ejecutar los procedimientos adecuados en el caso de que se produzca una situación crítica.

3.- Determinar las acciones de respuesta

Esta fase del plan implica tener muy bien definida una hoja de ruta con las siguientes acciones a llevar a cabo:

- Indicadores que marcarán el inicio del plan de contingencia.
- Secuencias de acciones que habrá que llevar a cabo en el orden preciso.

- Indicadores que permitan considerar que la situación ha quedado normalizada.
- Determinación de los registros y documentación necesaria para dejar constancia por escrito de las acciones que se han llevado a cabo.

4.-Mantenimiento del plan

Es necesaria la obtención de datos de ejecución del plan con el fin de actualizarse y mejorarse para incrementar su eficiencia en futuras ejecuciones.

Un Plan de Contingencia suficientemente elaborado permite retomar las actividades dentro de unos tiempos de recuperación adecuados, previamente definidos.

Esto permite volver a la actividad normal en un tiempo prudencial, antes de que se produzcan pérdidas de consideración, una cuestión que no tienen en cuenta ni prevén otros estándares y normas diferentes a la ISO 22301.

CARACTERÍSTICAS DE LOS TIEMPOS DE RECUPERACIÓN:

- Se deben conocer y definir con exactitud antes de elaborar el plan de contingencia.
- Los tiempos de recuperación deben encuadrarse en unos mínimos aceptables para poder reanudar la actividad dentro de unos márgenes que impidan que la empresa sufra daños económicos o de logística irreparables o muy importantes.

FASES DE LA IMPLANTACIÓN DE UN SGCN

Desde el diseño de la estrategia a la ejecución de un Plan de Continuidad del Negocio definido en un SGCN, y tomando como base el estándar ISO 22301:2012, la implantación y certificación del mismo es un proceso dividido en las siguientes partes:

1) Definición y gestión del riesgo. Se trata de un requisito previo que consiste en la identificación de los activos críticos y de los riesgos asociados.

2) Análisis de impacto. Es una de las partes más importantes del proceso y, básicamente, se trata de relacionar los procesos de negocio identificados con los impactos que se prevé que podrían provocar una eventual interrupción de cada uno de ellos. Para realizar este proceso suele ser necesario llevar a cabo entrevistas en profundidad con profesionales expertos en cada actividad o sector.

3) Desarrollo del plan de acción.

En primer lugar, se debe realizar una invocación por parte de la Dirección de las acciones que deben activarse para continuar con la actividad.

A partir de aquí, ya puede definirse la estrategia más adecuada para restablecer la situación al punto de partida; es decir, que el tiempo que pasa desde el inicio del incidente hasta que se recupere la actividad normal sea el mínimo posible.

Una vez tenemos la estrategia, el siguiente paso consiste en concretar las acciones que sean necesarias para recuperar la operatividad normal de la organización, con todos los procesos y circuitos funcionando a un nivel óptimo.

Por último, se deben realizar una serie de ensayos o pruebas con el fin de garantizar que estas acciones van a funcionar correctamente y cumplirán su objetivo en el momento de ponerlas en práctica en una situación real.

En el plan de acción o plan de contingencias debe constar:

- Los riesgos a controlar y la acción de reposición asociada a cada riesgo.
- Activos involucrados• Nivel de servicio exigido• Tiempo de respuesta• Recursos necesarios• Procedimientos y responsables

4) Monitorización, análisis y evaluación

Deben determinarse los objetivos y herramientas de monitorización, medición, análisis y evaluación, así como los períodos de desempeño y ejecución. Dicha monitorización debe estar basada en métricas que sirvan para evaluar, entre otros, los siguientes factores:

- Desempeño de los procesos
- Conformidad de los estándares internacionales
- Registro de los datos obtenidos

La evaluación se debe llevar a cabo mediante auditorías internas y auditorías externas.

- Auditorías internas

Las auditorías internas han de estar supervisadas por la Dirección o Gerencia de la organización, y su principal cometido es determinar la conformidad del SGCN con los requerimientos de la organización y de los estándares internacionales, en especial la norma ISO 22301.

A través de estas auditorías y revisiones periódicas, la organización puede lograr los siguientes beneficios:

- Comprobar si la estrategia definida es realmente eficaz para garantizar la continuidad del negocio.
- Implantar las correcciones precisas y necesarias para mejorar el alcance y la efectividad del SGCN.
- Comprobar y actualizar los diversos aspectos del SGCN: evaluación de riesgos, análisis del impacto, planes de continuidad y procedimientos relacionados.
- Mejorar la monitorización de todo lo relacionado con el SGCN.

Si se descubre una disconformidad relevante entre los objetivos definidos y la situación real en relación a los planes de acción relativos a la continuidad del negocio, deben llevarse a cabo los siguientes pasos:

1. Identificación de la disconformidad
2. Evaluación de la necesidad de poner en macha acciones correctivas
3. Ejecución de dichas acciones
4. Revisión de la efectividad de las acciones
5. Ejecución de los cambios que sean necesarios en el SGCN

- Auditorías externas

La ISO 22301 es una norma certificable, lo que implica realizar auditorías externas por parte de una empresa autorizada, revisables periódicamente, con el fin de conseguir y mantener dicha certificación.

La certificación sirve para demostrar a los clientes, proveedores y partes interesadas que nuestra empresa considera prioritario proteger los procesos esenciales que permitan, en todo momento, proveer de los productos y/o servicios necesarios a sus clientes.

5.5. INTEGRACIÓN ISO 27001 E ISO 22301

La norma ISO 27001 que vimos en el apartado anterior y la ISO 22301 están muy relacionadas, en concreto el Anexo A.17.1 de la ISO 27001 es el que hace referencia a la continuidad del negocio:

> A.17.1 Continuidad de la Seguridad de la Información
>
> La continuidad de la Seguridad de la Información debe formar parte de los Sistemas de Gestión de Continuidad de Negocio de la organización.
>
> A.17.1.1 – Planificación de la continuidad de la seguridad de la información
>
> A.17.1.2 – Implementar la continuidad de la seguridad de la información
>
> A.17.1.3 – Verificación, revisión y evaluación de la continuidad de la seguridad de la información
>
> A.17.1.1 Planificación de la continuidad de la seguridad de la información

DOCUMENTOS

- Política de continuidad del negocio
- Metodología para el análisis del impacto en el negocio

- Cuestionario sobre el análisis del impacto en el negocio
- Estrategia de continuidad del negocio
- Lista de actividades
- Prioridades de recuperación para las actividades
- Objetivos de tiempo de recuperación para actividades
- Ejemplos de escenarios de incidentes disruptivos
- Estrategia de recuperación de actividades

A.17.1.2 Implementar la continuidad de la seguridad de la información

La organización debe establecer, documentar, implantar y mantener:

- Controles de seguridad de la información en los procesos, procedimientos y sistemas de continuidad del negocio o de recuperación de desastres.
- Procesos y procedimientos para mantener los controles existentes de seguridad de la información durante una situación adversa.

DOCUMENTOS

- Plan de recuperación ante desastres
- Plan de continuidad del negocio
- Plan de respuesta ante incidentes
- Lista de ubicaciones para la continuidad del negocio
- Plan de transporte
- Contactos clave
- Plan de recuperación de actividades

A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

CONTROL

La organización debería comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.

Las organizaciones deberían verificar su gestión de la continuidad de la seguridad de la información:

- Ejecutando y probando la funcionalidad de los procesos, procedimientos y controles para la continuidad de la Seguridad de la Información asegurando que son consistentes con los objetivos de continuidad de seguridad de la información.
- Ejecutando y probando el conocimiento y la rutina para operar los procesos, procedimientos y controles de continuidad de la Seguridad de la Información, asegurando que su rendimiento es consistente con los objetivos de continuidad de seguridad de la información.
- Revisando la validez y efectividad de las medidas para la continuidad de la Seguridad de la Información cuando se produzcan cambios en la organización.

DOCUMENTOS

- Registro de incidentes
- Plan de prueba y verificación
- Formulario – Informe de prueba y verificación
- Plan de mantenimiento y revisión del SGCN
- Formulario de revisión post-incidente

6. ISO 27001 E ISO 27701

En agosto de 2019 se publicó una nueva norma relacionada con la familia ISO 27000. Especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Información de Privacidad en forma de una extensión a ISO/IEC 27001 y la ISO/IEC 27002 para la gestión de privacidad dentro del contexto de la organización.

Es aplicable a todos los tipos y tamaños de organizaciones, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro, que tengan implantado un Sistema de Gestión de la Seguridad de la Información.

Una organización que cumple con los requisitos de la ISO/IEC 27701 contará con evidencias documentadas del tratamiento de datos personales. Estas evidencias proporcionan a la organización garantías adecuadas de cumplimiento.

La certificación en la ISO/IEC 27701 junto con la certificación en la norma ISO/IEC 27001 implica contar con una evidencia fundamental en materia de cumplimiento normativo en privacidad de datos, según viene indicado en el GDPR en su artículo 24.3 al establecer, entre las obligaciones que pesan sobre los responsables del tratamiento de datos personales de las organizaciones, que:

> *la adhesión a […] un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.*

Por otro lado, certificarse en la ISO 27701 sirve para acreditar el cumplimiento de las obligaciones de privacidad desde el diseño y por defecto regulado en el artículo 25.3 de la GDPR.

7. BIBLIOGRAFÍA

ISO/IEC 27001: 2017

https://www.aenor.com/normas-y-libros/buscador-de-normas/UNE?c=N0058428

ISO/IEC 27002: 2017

https://www.aenor.com/normas-y-libros/buscador-de-normas/UNE?c=N0058429

ISO/IEC 22301: 2015

https://www.aenor.com/normas-y-libros/buscador-de-normas/UNE?c=N0054336

ISO/IEC 27701:2019

https://www.aenor.com/normas-y-libros/buscador-de-normas/iso/?c=071670

PARC CIENTÍFIC
VNIVERSITAT DE VALÈNCIA

Coordinadora de la edición: María Iranzo

Con el apoyo de

GENERALITAT VALENCIANA

IVACE
INSTITUT VALENCIÀ DE COMPETITIVITAT EMPRESARIAL

Síguenos en redes: