ARTICULO 197 BIS Y RECOMENDACIONES PARA LA PREVENCION DE LOS CIBERDELITOS CONTRA LA INTIMIDAD.

Manuel Angel Tevenet Gutiérrez
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Josep Cañabate Pérez

06/2019

FICHA DEL TRABAJO FINAL

Título del trabajo:	ARTICULO 197 BIS Y RECOMENDACIONES PARA LA PREVENCION DE LOS CIBERDELITOS CONTRA LA INTIMIDAD.
Nombre del autor:	Manuel Angel Tevenet Gutiérrez
Nombre del consultor:	
Fecha de entrega (mm/aaaa):	06/2019
Área del Trabajo Final:	Aspectos legales de la seguridad informática
Titulación:	*MISTIC*

Resumen del Trabajo (máximo 250 palabras):

Se pretende dar una visión general del estado general de la legislatura española en ciberdelitos, desglosar las amenazas más comunes, que se engloben en el articulo 197 Bis. Todas estas acciones se realizarán con el fin de ayudar, formar y concienciar a todo aquel que pueda leer este TFM en el ámbito actual de los ciberdelitos.

Como problema objetivo se plantea el creciente grado de importancia que tiene en la sociedad actual el mundo cibernético y por consiguiente el grado de exposición que tiene la ciudadanía en este espacio.

Para conseguir desgranar esta situación se presentarán los ciberdelitos más populares actualmente que violen el artículo 197 CP bis del Código Penal, así como los más importantes a nivel histórico. También se tratará de comprender como la ley vigente trata de combatir esta actitud delictiva. Para ello nos valdremos de casos reales y cercanos a la vez que cotidianos para tomar una visión espacial de todo este panorama.

El enfoque de este TFM se realizará desde el punto de vista jurídico de la Ley vigente en España. En algún caso en concreto y según se necesite se acudirá a la Ley Europea. Llegando de esta manera al objetivo principal del trabajo que es proporcionar al lector una serie de prácticas y recomendaciones para la prevención de los delitos contra la intimidad previstos en el mencionado artículo.

Abstract (in English, 250 words or less):

It is intended to give an overview of the general state of the Spanish legislature in cybercrimes, break down the most common threats, which are included in Article 197 Bis. All these actions will be carried out in order to help, train and raise awareness of anyone who can read this TFM in the current field of cybercrime.

The objective problem is the growing importance of the cybernetic world in today's society and therefore the degree of exposure that citizens have in this space.

In order to get the best out of this situation, the most popular cybercrimes currently violating Article 197 of the Criminal Code, as well as the most important at the historical level, will be presented. It will also try to understand how the current law tries to combat this criminal attitude. For this we will use real and close cases at the same time as everyday to take a spatial view of this whole panorama.

The focus of this TFM will be carried out from the legal point of view of the current Law in Spain. In some specific case and according to need, we will turn to European Law. Reaching in this way the main objective of the work that is to provide the reader with a series of practices and recommendations for the prevention of crimes against privacy provided in the aforementioned article.

Palabras clave (entre 4 y 8):

Ciberdelito, amenaza, hacker, hacking, concienciación, legislación.

INDICE.

Contenido

1. INTRODUCCION.

Para el presente TFM se pretende elaborar una herramienta de información sobre la legislación actual tanto nacional como internacional en ciberdelitos contra la intimidad y que a su vez sirva como herramienta de prevención y concienciación para todo aquel que lo consulte.

Se realizará un estudio del artículo 197 Bis del Código Penal que tras la reforma del 2015 es el que recoge este tipo de delitos. Se analizarán sus defectos y virtudes desde el punto de vista ético y técnico y se comentarán las posibles mejoras que podría tener la nueva ubicación del mismo dentro del Código Penal.

Se va a analizar el nivel de concienciación de la sociedad ante este tipo de delitos a la vez que se analizarán diferentes métodos para aumentar el mismo. También se reportarán una serie de consejos o buenas prácticas con el objetivo de mejorar la cibereducación y prevenir el ser víctimas de los ciberdelitos en la medida de lo posible.

Por último se desglosarán las principales compañías en ciberseguridad a nivel mundial y se destacan sus aportaciones más relevantes en materia de prevención y riesgos cibernéticos.

1.1 Contexto y justificación del Trabajo

Estamos siendo testigos de primera mano de un hito en el desarrollo de la humanidad. La revolución tecnológica ha empezado, y en las próximas décadas asistiremos a un giro radical en nuestro comportamiento cotidiano, en el que numerosas actividades tradicionales van a ser sustituidas o compatibilizadas con la utilización de máquinas.

Con esta revolución se generarán numerosas transformaciones en la sociedad, entre las que por ende se incluirán nuevas formas de delinquir. Los métodos tradicionales para practicar el delito siempre van a permanecer en nuestra sociedad, pero a éstos se van a unir cada vez en mayor medida las nuevas formas de ciberdelincuencia.

Existen múltiples clasificaciones para catalogar los delitos cometidos por medios cibernéticos. En la que se expone a continuación, se puede sacar en claro la importancia que toma la lucha contra esta forma de delinquir. De esta manera se pueden distinguir los siguientes.

Personas aisladas que cometen infracciones con fines exclusivamente individuales (hackers, crackers, etc.).

También podemos catalogar el Crimen Organizado, uniones de personas en infraestructuras más o menos desarrolladas, que de forma organizada se sirven de los sistemas informáticos para su finalidad, que suele ser económica o relacionada con ésta.

Ciberguerra, en esta vertiente para alcanzar los fines específicos que se pretendan conlleva la intervención de los estados. La finalidad y los medios empleados suelen ser muy diversos ya que pueden diversificarse en su origen, tales como la obtención de información, la alteración de la economía de un estado con consecuencias económicas

en un tercero (podemos imaginar el ataque a una bolsa nacional de gran importancia o a un puerto de mayor o menor actividad), y en definitiva, cualquier tipo de amenaza a infraestructuras críticas.

Otra vertiente es la que se está desarrollando a través de las organizaciones terroristas que además de los métodos tradicionales de terrorismo ahora practican otra de manera cibernética, el ciberterrorismo. Esta adicción de delitos informáticos tiene la finalidad de contribuir a su finalidad de propaganda y alteración del orden, principalmente mediante ataques dañinos sin especial finalidad económica.

En el ámbito nacional ciertos autores dudan del automatismo del legislador nacional a la hora de incorporar a nuestro ordenamiento jurídico las normas internacionales, con la excusa de satisfacer compromisos ya asumidos en otras sedes.

Además de este automatismo, verdaderamente se echa en falta es que los legisladores españoles realicen un esfuerzo en adaptar las normas internaciones a las particularidades que presentan nuestras leyes ya que como se verá en próximos capítulos del trabajo, sencillamente se están trasladando la normativa nacional sin hacer ningún tipo de esfuerzo en armonizarlas con el sistema jurídico nacional. De esta manera aumenta de manera notable el esfuerzo a realizar por el intérprete con el consiguiente riesgo de interpretaciones heterogéneas con el consiguiente detrimento de la seguridad jurídica.

La principal norma en la materia es el Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, pues inspira la normativa europea y constituye la referencia absoluta en las formas de lucha contra la ciberdelincuencia desde su elaboración, y ello pese a la tardía entrada en vigor para España (1 de octubre de 2010, de acuerdo con el Instrumento de Ratificación publicado en el BOE el 17 de septiembre de 2010). A esto se ha de añadir un informe explicativo, que aunque no es un instrumento que ofrezca una interpretación autorizada, sí que da criterios interpretativos importantes.

Tras este primer paso, no se introducen novedades significativas en el código penal hasta el año 2015 con una nueva reforma. Con esta nueva reforma se introducen gran cantidad de novedades aunque no sin cierta polémica en la parte general. En la parte especial aunque no de manera tan determinante también se presentan alteraciones.

Con esta nueva reforma hay varios delitos que se ven afectados, entre los cuales se encuentran los delitos contra la intimidad, de los cuales se han incorporado no solo modificaciones formales si no también sustanciales.

En materia de tutela la única novedad del bien jurídico de la intimidad venia representada por la introducción de una figura delictiva consistente en la difusión no autorizada de imágenes, grabaciones y demás material audiovisual obtenido bajo el consentimiento de la víctima, aunque a continuación se añadieron otras figuras delictivas en el ámbito del llamado delito de intrusismo informático, del cual también se informará en este trabajo, consistente en interceptar ilegalmente transmisiones no publicas entre sistemas por un lado y por otro facilitar los instrumentos para este intrusismo.

Por último se introdujo un tipo cuando la conducta delictiva viene dada por la utilización de datos personales de otra persona como vía para ganarse la confianza de la víctima y así atentar contra su intimidad.

1.2 Objetivos del Trabajo

Como problema objetivo se plantea el creciente grado de importancia que tiene en la sociedad actual el mundo cibernético y por consiguiente el grado de exposición que tiene la ciudadanía en este espacio. En el mundo actual un usuario ya no solo se conecta a través de su PC, si no que existen múltiples dispositivos en nuestra vida cotidiana conectados a la red. La escalada en cuanto a delitos que se está produciendo en los últimos años y que no para de crecer aumentando en número y en complejidad hace que nos planteemos también el problema que con lleva el desconocimiento que pueden tener los usuarios a la hora de cometer un ciberdelito, que este se pueda efectuar por error, desconocimiento o bien por simple mala suerte.

De esta manera se planteará como objetivo principal la elaboración de unas recomendaciones para la prevención de los delitos contra la intimidad previstos en el mencionado artículo.

También se desarrollarán los siguientes objetivos específicos:

- El estudio del artículo 197 bis y de los supuestos que contempla
- Descripción de las amenazas y riesgos más frecuentes asociados con el delito.
- Analizar el grado de concienciación de la población y las empresas en relación a los riesgos de sufrir los ciberdelitos relacionados.
- Comparar recomendaciones que puedan hacer instituciones oficiales como INCIBE, etc.

1.3 Enfoque y método seguido.

El enfoque de este TFM se realizará desde el punto de vista jurídico de la Ley vigente en España. En algún caso en concreto y según se necesite se acudirá a la Ley Europea.

En cuanto al enfoque ético lo se tratará en cada apartado al desglosar los principales tipos de ciberdelitos y en el daño que pueden causar a la víctima. Según sea conveniente trataremos de empatizar con la víctima y también de ver las causas o motivos éticos que pudiera tener el atacante si los hubiera. Llegando de esta manera al objetivo principal del trabajo que es proporcionar al lector una serie de prácticas y recomendaciones para la prevención de los delitos contra la intimidad previstos en el mencionado artículo.

1.4 Planificación del Trabajo.

Debido al retraso con el que se empieza el TFM se han adaptado los plazos para acabar en el tiempo previsto. Esto se ha conseguido acortando algunas fases del proyecto y solapándolas con la intención de complementarlas y finalizar en el tiempo estipulado.

Para acabar en tiempo y forma el TFM se han tenido en cuenta semanas con días de trabajo de lunes a sábado, aunque presumiblemente los domingos también se trabajara sobre el TFM. También se trabajará en el mismo en las semanas festivas tales como Semana Santa y Feria a tiempo completo lo cual ayudará en la tarea de acortar plazos para entregar el TFM a principios de junio.

Se adjunta diagrama de Gantt junto con el documento para entender su desglose y solapamiento de tareas.

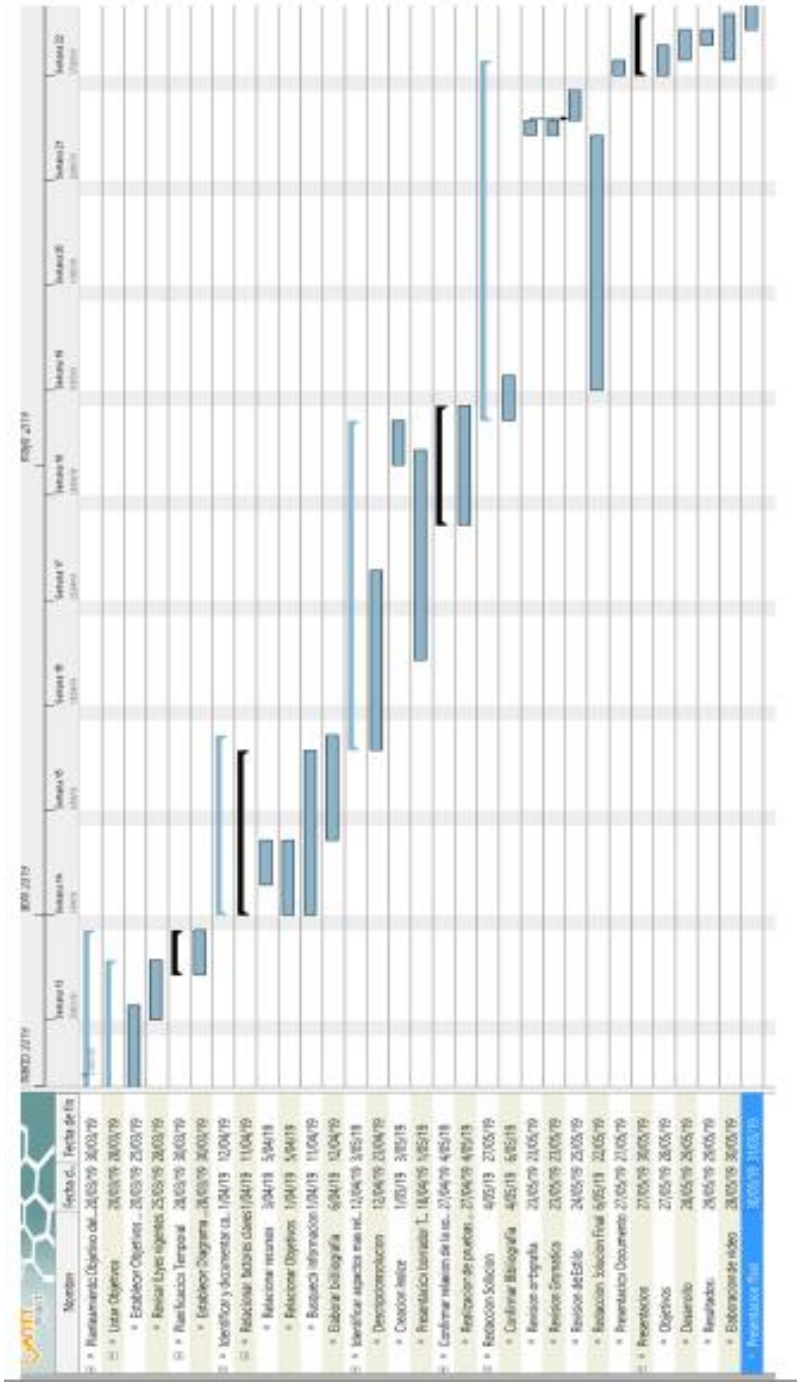

Ilustración 1 Diagrama de Gantt del TFM

2. EL DELITO INFORMATICO.

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de los sistemas informáticos y ordenadores, lo que ha propiciado a su vez la necesidad de regulación por parte del Derecho.

A nivel internacional se considera que no existe una definición propia del delito informático, aunque hasta el momento muchos han sido los expertos que han centrado sus esfuerzos en este tema, y aún sin existir una definición universal para este tema, se han formulado conceptos funcionales atendiendo a las necesidades nacionales en cuestión.

Cabe destacar que la delincuencia informática se apoya en el delito realizado mediante el uso del ordenador a través de redes telemáticas, y la interconexión de estos computadores, aunque bien es cierto que éste no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales, afectando finalmente al grueso de la sociedad.

A partir de estos principios, en el presente trabajo se entenderán como delitos informáticos todas aquellas conductas ilícitas susceptibles de ser penadas por el Derecho Penal, que hacen un uso indebido de cualquier medio informático.

2.1 Clasificación de los delitos informáticos.

Según Julio Téllez Valdés podemos clasificar los delitos informáticos desglosándolos en dos grupos, si sirven como instrumento o si actúan como fin u objetivo.

Si nos centramos en la clasificación que los cataloga como instrumento o medio, se pueden encontrar las conductas criminales que se sirven de los ordenadores como método o medio del acto con el que se realiza el incumplimiento de la ley.

En esta clasificación podemos destacar actos ilícitos tales como:

- *Falsificación de documentos.*
- *Modificación, lectura o sustracción de datos.*
- *Modificación de datos contables.*
- *Acceso a sistemas violando códigos de entrada.*
- *Uso no autorizado de programas.*
- *Infección de sistemas a través de virus informáticos.*

En cuanto a la otra vertiente, es decir, actuando como fin u objetivo, podemos englobar acciones que actúa contra ordenadores accesorios u otros programas:

- *Destrucción de software.*

- *Uso de programas con el fin de bloquear sistemas.*
- *Perjuicio de sistemas de almacenamiento.*
- *Daño físico o secuestro a sistemas y sistemas de almacenamiento con fines delictivos.*

Si nos centramos en el comportamiento que conlleva el realizar un delito informático, en su libro Leyes y negocios en Internet, Oliver Hance afirma que hay tres tipos de actitudes que pueden adoptar los usuarios afectando negativamente a los sistemas.

La primera acción de un delito informático es el *Acceso no autorizado*, bien sea de manera voluntaria o involuntaria. Si la conexión se realiza de manera no voluntaria, es el usuario el que decide permanecer en la red cometiendo el acto ilícito.

Una vez conectados es cuando se realizan *los daños o el trasvase de material maligno*. Este comportamiento se manifiesta bien a través de del robo de información o bien promoviendo su circulación como puede ser mediante el uso de virus o gusanos. Esto es lo que se define como piratería.

Por último, se puede realizar la *intercepción no autorizada de datos o comunicaciones* las cuales no están dirigidas a ese usuario.

2.2 Tipos de Delitos informáticos.

A continuación se desglosarán los principales tipos de delitos informáticos que están reconocidos por la ONU tales como fraudes, falsificaciones o daños y modificaciones.

2.2.1 Fraudes a través de la manipulación de equipos.

Este tipo de fraude engloba diversas maneras de efectuar el acto ilícito ya que según el elemento que se manipule o bien el tipo de datos se puede distinguir una forma de realizar el acto u otra.

Cuando se trata de *manipulación de datos de entrada*, o sustracción de datos como es más comúnmente conocido este tipo de fraude se detecta de manera más rápida al igual que es más fácil de cometer dado que no es necesario poseer unos conocimientos técnicos muy avanzados.

Es posible también *manipular los datos de salida*. Cuando se establece como objetivo el propio funcionamiento del sistema informático. Actualmente se puede fijar el foco en la manera en que ha evolucionado el fraude en los cajeros automáticos ya que actualmente no se realizan a través de tarjetas bancarias si no que hoy día se pueden manipular las instrucciones de la maquina con el fin de la obtención de datos.

2.2.2 Falsificaciones informáticas.

Este tipo de delito suele tener fines diversos e incluso injustificables desde el punto económico o político, más allá que el de dañar a otro usuario o entidad.

Las falsificaciones informáticas como objeto radican en la alteración de datos de documentos que se almacenan en los equipos atacados.

También es común que se utilice la *falsificación como instrumento*, esto suele ocurrir con fines comerciales.

2.2.3 Modificaciones de software.

Cuando hablamos de este tipo de delito si se pude intuir un fin más dañino que los anteriores tanto a nivel de sistemas, como de equipos y entidades.

Cuando se habla de distintas modificaciones de software muchas veces se puede deber a un acto de *sabotaje informático*, el cual se realiza eliminando o modificando de manera no autorizada datos o funciones del equipo con el fin de dificultar el correcto funcionamiento del mismo. Los actos de sabotaje se pueden efectuar a través de virus, gusanos o bombas lógicas.

Como en todos los actos delictivos informáticos, la mayoría de estos vienen precedidos por un *acceso no autorizado*, en este caso a los servicios o sistemas del equipo atacado. El motivo de este acceso es diverso y pueden radicar desde la curiosidad o el demostrarse a sí mismo sus conocimientos hasta el sabotaje o espionaje.

La *piratería o reproducción ilegal* de programas de protección. Esta acción supone casi en la totalidad de las veces pérdidas económicas para la compañía propietaria y en algunos países se ha tipificado como delito y se ha penado. En otros por el contrario no, ya que se establece que el bien es la propiedad intelectual.

Si se atiende a la acción que se efectúa a la hora de cometer el delito, hay varios grupos en los que se podría dividir.

Se vuelve a clasificar primeramente el *acceso no autorizad*o mediante el uso ilícito de credenciales sin el consentimiento del propietario.

La *destrucción de datos* a través de gusanos, virus, bombas lógicas y demás elementos dañinos que pudieran afectar al sistema.

Uso no autorizado de la información de una base de datos *infringiendo el Copyright*.

Las *estafas electrónicas* y la *intercepción de correo electrónico* mediante compras en la red y la lectura de correo ajeno.

Se puede engañar en la actividad bancaria realizando *transferencias de fondos*.

Por otro lado, la red puede dar cobertura para que se realicen otro tipo de delitos más variados como son los que se refieren a continuación.

Espionaje, mediante el acceso no autorizado a sistemas gubernamentales o de grandes compañías.

Exaltación del terrorismo mediante mensajes anónimos con consignas, organización y transmisión de planes por parte de las bandas terroristas.

La red también da soporte al *narcotráfico* de manera económica, organizativa y estructural facilitando el blanqueo de dinero, la transmisión de fórmulas para estupefacientes y la coordinación logística para entregas y recepciones.

3. EL ARTÍCULO 197 BIS.

El artículo en el que se basa el grueso de este trabajo y sobre el que se pretende dar un mayor grado de concienciación y conocimiento es el artículo del Código Penal 197 Bis. Este artículo recoge la conducta básica del hacking y establece lo siguiente.

"El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años".

De esta manera, se puede confirmar que este artículo engloba tanto el acceso no autorizado a un sistema como la permanencia posterior en el mismo, esto, puede desembocar según Queralt Jiménez[1] en la tipificación de un acto preparatorio punible por cuanto la intrusión por intrusión, aunque es posible, al resultar inútil, no es fácil que mueva o despierte muchos ánimos criminales sin tener otro fin más allá.

Para contemplar de manera completa el alcance del artículo 197 Bis del Código Penal se requieren de otros requisitos que se analizarán a continuación a través de las conductas ilícitas que éste recoge tales como la vulneración de las medidas de seguridad establecidas para impedir un acceso no autorizado y que se acceda al sistema informático o bien a parte del mismo.

De esta manera se puede encontrar un segundo grupo de conductas que son reguladas en el mismo artículo que son las hacen referencias a la permanencia o mantenimiento en el sistema informático, aunque este comportamiento según se ha manifestado no son propiamente pertenecientes a un acceso ilícito al sistema. De esta manera, el mantenimiento es el acto de mantenerse, es decir, dar continuidad a lo que se está ejecutando una vez realizado el acceso ilícito.

Así, el mantenimiento al que hace referencia el artículo 197 Bis del Código Penal necesita un acceso anterior ejecutado de manera ilícita teniendo la voluntad en contra de quien tiene el legítimo derecho de acceso y de exclusión al sistema.

Como resultado se tiene la necesita de delimitar todos los conceptos a los que hace referencia el artículo con el fin de comprender el verdadero alcance del mismo. De esta manera se empezará por los sujetos ya que es necesario conocer las conductas a las que se refiere el artículo para plantear diferentes situaciones que dan lugar a esa conducta y como penarla o evitarla.

3.1 Los sujetos.

Orts Berenguer y González Cussac[2] advierten que el DP solo se centra en las conductas de los sujetos que realizan el acto delictivo si lo que se considera es el concepto de acción o incluso la definición del delito.

[1] QUERALT JIMÉNEZ, J. J., Derecho penal español ..., p. 338.
[2] ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., Compendio de Derecho ..., p. 305.

Se puede considerar que el sujeto activo es la persona que realiza el acto delictivo, de tal manera, los objetos de los que se sirve son el sujeto activo secundario, de esta manera, podemos considerar que el sujeto pasivo es la persona o sistema sobre quien recaen las acciones delictivas del sujeto activo. Aunque hay autores que prefieren reservar este último término para el objeto material del delito.

Aunque de manera habitual se utilizan de la misma manera los términos sujeto activo y autor, el sujeto activo es quien realiza el comportamiento típico mientras que autor tiene la responsabilidad criminal por el hecho implícita, de esta manera según Orts Berenguer y González Cussac[3], el sujeto activo constituye una parte más del tipo de acción, es decir, el sujeto de la disposición que lo define, integrándose en el campo normativo, no real, al que pertenecería el autor.

3.1 El sujeto activo.

Hay varias vertientes en cuanto a la definición del sujeto activo. Hay quienes opinan que el sujeto activo en un delito de hacking puede ser cualquiera, catalogándose, así como un delito común dentro del Código Penal, aunque la vertiente más usual y como indica Miró Llinares[4], lo más común es que la persona quien realiza el acceso no autorizado posea conocimientos informáticos avanzados ya que el acto que realiza se presupone de una dificultad tecnológica compleja.

De manera más precisa, se pude afirmar que el sujeto activo será la persona que acceda a parte o todo un sistema informático sin haber sido autorizado por la persona que tiene el legítimo derecho a acceder, autorizar o excluir el acceso a otros. Esta autorización se hace extensible para la organización propietaria del sistema.

3.1.1 El sujeto pasivo.

El sujeto pasivo si se sigue el mismo razonamiento que en el anterior apartado también puede ser cualquiera, aunque para el sujeto pasivo hay que concretar que debe ser el titular del sistema informático sobre el que se lleva a cabo del acto ilícito de acceso o mantenimiento. Esto engloba también además del acceso, la interferencia o intercepción que no haya sido autorizada por el propietario o titular del sistema.

Anarte Borrallo y Doval País[5], suponen el caso en el que el titular del sistema no es la misma persona cuyos datos o intimidad se puede ver vulnerada por el acceso ilícito. De esta manera concluyen que, si la persona que accede es la titular del derecho de intimidad o datos afectados, no cometería ningún acto delictivo siempre que el sistema no almacene datos de terceros, mientras que, si es otra persona la que accede al sistema que tiene un titular y unos datos pertenecientes a otra persona, cometería un solo delito relacionado tan sólo con el titular de los datos y no del sistema.

Aunque en el artículo 197.3 del Código Penal en su primera redacción del año 2010 ya se hacía referencia al acceso ilícito a sistemas informáticos, con la reforma de la LO 1/2015 parece que el planteamiento de seguridad e integridad del sistema se trata de preservar como bien jurídico, protegiéndolo y penando su acceso independientemente de que el sistema contenga datos de un tercero o del mismo titular del sistema.

[3] ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L., Compendio de Derecho penal ..., p. 305.
[4] MI LLINARES, F., “Los Delitos Informáticos ...", p. 147.
[5] Ibid., p. 17.

Si el sistema al que se accede contiene datos de un tercero distinto al titular del sistema, el sujeto pasivo del delito seguirá siendo el titular del sistema según el artículo 197 bis Código Penal, aunque podría existir otro bien jurídico comprometido si se accediera, modificara o eliminara esa información del tercero en cuestión o se tuviera la intención de desvelar algún tipo de secreto.

3.2 Conductas típicas.

Atendiendo a lo expuesto hasta ahora, los comportamientos o conductas que puede manifestar el infractor en cuestión son muy diversas y pueden comprender desde los supuestos usos de generadores de claves o cracks hasta el uso de snifers utilizados como programas de captura de tramas de información. según esta afirmación de Miró Llinares[6], a través de este tipo de software sería viable el acceso a servidores donde se hallen los correos electrónicos lo que conlleva un acceso no autorizado a un sistema o parte del mismo.

Asimismo, el fragmento del artículo que dice "*o facilite el acceso*" es una modificación novedosa que aporta el artículo 197 BIS. Al igual que el resto del artículo, esta novedad fue introducida con el fin de superar las limitaciones que hasta ese momento presentaba la legislación vigente y presentar respuesta a los delitos informáticos que empezaban su escalada de manera notable.

Gramaticalmente el fragmento "*facilitar el acceso*" no presenta problemas de interpretación, sin embargo en el artículo 197 Ter sí que puede llevar a cierta confusión con las conductas ya que se establece que:

"Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis: a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".

Como se puede comprobar, en este apartado también está prevista la facilitación del acceso a terceros con el fin de cometer el acto delictivo. La diferencia radica en que el artículo 197 Ter se hace referencia a facilitar el uso de instrumentos para conseguir el acceso, bien sea software la consecución de una contraseña, datos o información o algún tipo de código de acceso. Aunque esta ambigüedad en cuanto a facilitar "datos similares" a "una contraseña de ordenador" o "un código de acceso" puede plantear problemas de delimitación en la práctica entre estas conductas y la de facilitar el acceso prevista en el artículo 197 bis.

Al incluir este tipo de conductas de facilitar el acceso en la LO 1/2015 se tipifica de manera expresa que estos actos de cooperación suponen actos de autoría. Así, Colás Turégano [7]indica que, en estos casos se produce una criticable ampliación de la autoría a supuestos que con anterioridad a la reforma se habrían considerado como participación. Por ello, para estos casos deberá entenderse que se ha producido un

[6] MIRÓ LLINARES, F., El cibercrimen ...,p. 308.
[7] COLÁS TURÉGANO, A., "Nuevas conductas delictivas ...", p. 676.

efectivo acceso, por cuanto no tendría sentido la citada ampliación del ámbito punible si no se tuviese lugar ese acceso, además de que produciría problemas de delimitación respecto a las conductas del artículo 197 Ter Código Penal.

4. EL DELITO DE ALLANAMIENTO INFORMATICO.

El intrusismo o espionaje informático recibe en el Código Penal la denominación de Allanamiento Informático. Este concepto se introdujo en el Código Penal en la Reforma por la LO 5/2010, aunque de manera más escueta que el desarrollo actual ya que solo introducía el tipo básico de delito, la responsabilidad de las personas y el agravamiento cuando se trataba de actos cometidos por grupos u organizaciones.

Con la reforma efectuada en 2015 se pretendía llegar a diferencias de manera clara los delitos de revelación o descubrimiento de secretos en su vertiente de ataque contra la intimidad personal del de allanamiento informático básico. Aunque actualmente esta intención puede considerarse que solo quedó en eso, ya que no se podría considerar del todo correcta ya que se podría haber concreta estableciendo un capítulo integro para ello en la regulación de delitos informáticos.

Volviendo al artículo que nos ocupa, de manera completa dice así:

«1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.»

De esta manera se puede confirmar que el artículo se compone de dos apartados bien diferenciados ya que en el primero recoge lo que en la reforma de 2010 se describía en el 197.3, con lo que se pretende que el artículo 197 se enfoque principalmente a casos de revelación de datos que afecten de manera directa a la intimidad personal diferenciando así de los casos que afecten o supongan un ataque contra la privacidad pero por ende no tengan un efecto directo en la intimidad de ninguna persona. De esta manera se pretende corregirla ubicación del hacking en Código Penal ya que fue ampliamente criticada, aunque hay que reconocer que estas críticas aún tienen fundamento ya que dicho problema no se ha resuelto de manera completa por lo que siguen existiendo voces discordantes en pos de una nueva reforma del Código Penal.

Si se centra la atención en el apartado segundo del artículo, se puede encontrar un acto delictivo no descrito en la anterior reforma de 2010 el cual lleva estipulado una pena de tres meses a dos años de prisión o una multa de tres a doce meses. Estas penas pueden ser sentenciadas a quien mediante el uso de instrumentos técnicos o demás herramientas intercepte transmisiones privadas sin estar autorizado para ello. Estas transmisiones se pueden producir desde, hacia o dentro de un sistema de información, incluyendo las emisiones electromagnéticas que se produzcan. Esta nueva incorporación al Código Penal es resultado de la asimilación por parte de España del Convenio sobre Cibercriminalidad o Convenio de Budapest de 2001, aunque en este convenio sí que aparece tipificado entre los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos y no como delito contra

la intimidad. De esta manera las criticas anteriormente mencionadas sobre la ubicación dentro del Código Penal de este tipo de delitos serian extensibles ya que no englobaría todos los supuestos posibles ni valdrían las mismas interpretaciones.

El delito de descubrimiento de secretos informáticos, el cual podemos hallarlo tipificado en el artículo 197.2, mantiene su redacción original desde 1995 por lo que se puede afirmar que ha quedado obsoleto ya que continua con un tipo de redacción compleja y confusa:

Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

De esta manera, según el artículo, se hace necesario que la persona que se apodera, utiliza o modifica datos privados de otra ha de ser distinto de la persona a la que se quiere perjudicar, además, distinta al titular de los mismos. No obstante, no tiene sentido no contemplar que el tercero sea titular de los datos a los que se accede, es más, surgen voces que afirman que el legislador solo debería haber redactado el artículo pensando en ésta. De esta forma, de manera mayoritaria se tiende a afirmar que lo más correcto sería interpretar que bajo la referencia de tercero se debería englobar a cualquier persona distinta del sujeto activo, es decir que sufra las consecuencias del acto delictivo, incluido el titular de los datos. Entre los partidarios de esta corriente de interpretación integradora se encuentra entre otros el Tribunal Supremo.

Hay que realizar el esfuerzo de no confundir las conductas contempladas en los dos apartados del artículo 197, pues aunque algo difusas, entre ambos existen diferencias. La primera diferencia radica que en el apartado primero no se necesita actuar para revelar secretos o vulnerar la intimidad de un tercero, por lo que por ejemplo, la intercepción de una comunicación vía Skype ya no quedaría impune. Además en el primer apartado, lo que se persigue y castiga es la interceptación de transmisiones del titular de la información vulnerada, es decir la intimidad vulnerada mientras que en el otro el objetivo son las transmisiones no públicas de datos que se produzcan desde, hacia o dentro de un sistema de información, siendo ésta otra diferencia entre ambas conductas típicas, aunque no un obstáculo a aplicar el artículo que estamos analizando en el caso puesto de ejemplo, pues las llamadas a través de Internet tienen tal consideración. Otra diferencia puede radicar en que no se habla de ejecutar el acto sin el consentimiento del titular de los datos, si no sin estar autorizado.

Como se puede comprobar es dificultoso distinguir que modalidades de conducta recoge cada apartado del artículo que se analiza en el trabajo aunque se puede afirmar que el primero sanciona el apoderamiento, la utilización o modificación de los datos registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado, mientras que en el segundo se castiga el acceso a los mismos y, de nuevo, su alteración o modificación.

Dada la multitud de vertientes y maneras de interpretar el artículo que hay, ninguna de las propuestas de solución que se han presentado han resultado convincentes ni se han aceptado de manera general. Una de las más aceptadas se centra en el objeto material sobre el que recaen las conductas antes descritas radica en que las conductas

del primer inciso lo serían los datos reservados de carácter personal o familiar que se encuentran registrados, mientras que cuando en el segundo inciso se habla de «los mismos» seria para referirse no a los datos reservados sino a los ficheros, soportes y archivos en los que éstos están registrados. Así lo entendieron Carbonell Mateu y González Cussac[8], estos afirman que de no hacerlo de esta manera se estaría tipificando dos veces de manera que se reiterarían las conductas descritas. Debe tenerse en cuenta que desde la Universidad de Sevilla, los Catedráticos de Derecho Penal han cambiado de opinión y ahora afirman que en ambas partes del artículo el objeto sobre el que han de recaer las diversas modalidades de la conducta es idéntico: datos reservados de carácter personal o familiar ajenos.

4.1 El bien jurídico protegido.

En este apartado se estudiará el artículo desde al análisis del bien jurídico protegido, en comparación directa con el artículo 197 del Código Penal.

El artículo sobre el que se realiza el presente trabajo pretende proteger la intimidad personal, tipificando el acceso a transmisiones y a fuentes de información determinadas que tienen un objeto final claro que es el de descubrir secretos o vulnerar la intimidad de otra persona u organización. Esto se recoge en el primer apartado, mientras que en el segundo se castiga el acceso a fuentes de información que contengan información de carácter personal o familiar. En ambos casos, la determinación del bien jurídico protegido queda clara, siendo en el primer caso la intimidad personal y en el segundo el derecho a la protección de datos reservados de carácter personal.

Ante estos tipos de conductas y bienes, el artículo 197 Bis pretende salvaguardar la seguridad en el tráfico informático mediante la protección de la integridad del sistema de información. En este punto, la reforma de la LO 1/2015 supone una mejora de la redacción del tipo gracias a la ubicación aunque no aun del todo clara, sí que mejorada; por la exposición de motivos y por la explicación de las finalidades pretendidas.

4.2 Tipos de amenazas.

En el siguiente apartado se va a proceder al análisis del artículo 197 Código Penal a partir del tipo de amenazas que pretende combatir o penar y sobre las que pretende tener alcance.

4.2.1 Acceso, mantenimiento y facilitación ilícitos.

En la redacción del artículo con la reforma de 2015 se mantiene la tipificación ya escrita del acceso y mantenimiento en el sistema sin estar autorizados aunque se añade la conducta de facilitación de acceso al sistema.

El mantenimiento no autorizado en el sistema, cuando se ha exigido el abandono del mismo por alguien que tenga el legítimo derecho de exclusión, desemboca en el delito de allanamiento informático. En resumen, necesita de una voluntad expresa de

[8] Ibidem, segunda edición, 2008.

exclusión del sistema por alguien legitimado para ello, lo cual viene legitimado por el titular del mismo.

Como se aprecia en el primer párrafo, la principal novedad está en que se tipifica la conducta de facilitar el acceso al sistema. Esto aunque de manera indirecta al no ser quien cometa el acto ilícito supone una forma de participación en el mismo. Así, se equipara la autoría a la complicidad con el objetivo de poner en su justa medida de gravedad todas las conductas que conlleven la puesta en riesgo de las infraestructuras del sistema.

Esta conducta de facilitar el acceso no debe interpretarse desde un punto de vista técnico ya que lo que se produce, tal y como afirma Bermúdez González[9], es la respuesta ante una petición de información que de otro modo no se habría producido. Si ampliamos la interpretación se podría describir en esta afirmación todo el comportamiento de obtención de información proveniente de un sistema, siendo indiferente su contenido, y sea bien de entrada o de respuesta del sistema.

Como se puede comprobar hay multitud de interpretaciones y voces discordantes en demasiados supuestos como para que se pueda afirmar que la legislación actual es clara de cara al legislador, personas jurídicas, procesados y víctimas. De esta manera, se ha de ser prudente a la hora de adoptar una actitud sancionadora ya que como se acaba de indicar hay demasiados supuestos en los que los criterios interpretativos pueden variar.

Así pues, se puede afirmar que el acceso ilícito recoge la simpe intromisión no autorizada en un sistema informático, piratería o hacking y también cracking o sabotaje informático.

De esta manera, también se puede afirmar que el acceso ilegitimo no comprende el acceso libre o el acceso no autorizado por desconocimiento, en este caso se caería en un error de tipo. Tampoco está recogido el acceso a una página web, ya sea directamente o mediante enlaces.

4.2.2 Vulneración de las medidas de seguridad.

Se hace imprescindible que existan medidas de seguridad para contener el acceso no autorizado al sistema informático, ya que un acceso a un sistema que no tiene medidas de seguridad además no entrar dentro de la normalidad, no tendría manera de ser penado. El problema que se encuentra en esta situación es el nivel de las medidas de seguridad, es decir, que estas han de tener un mínimo exigible ya que como se ha afirmado antes, resulta difícil penar un acceso no autorizado donde el usuario no ha adoptado ningún tipo de medidas para el control de acceso.

Así, no es lo mismo obtener acceso a un sistema protegido con una clave predeterminada y común (la típica serie de ceros o de números ordenados), o con una clave automatizada pero fácilmente obtenible de manera lógica o con herramientas automatizadas, o con un sistema de encriptamiento que este obsoleto en estos momentos.

[9] BERMÚDEZ GONZÁLEZ, J.A., Descubrimiento de secretos e intrusiones informáticas. Centro de Estudios Jurídicos, Madrid 2016, pág. 19.

Se hace necesario así, conocer quien está a cargo de la seguridad del sistema y que tipo de sistema es.

En sistemas domésticos hay que tener en cuenta que el nivel de protección no suele ser de un nivel extremadamente alto. Es difícil exigirle a una persona común con una preparación limitada en la informática que tenga correctamente configurado su firewall, actualizado de manera completa su sistema operativo y antivirus, el cifrado de los datos del disco duro…sí que es recomendable un mínimo exigible y al menos contar con las contramedidas necesarias para conocer la identidad del atacante.

4.2.3 El acceso por cualquier medio o procedimiento.

En el artículo 197 Bis podemos encontrar la expresión de acceso por cualquier medio o procedimiento. La interpretación de esta expresión ha de ser de manera atenta, ya que puede parecer una expresión genérica utilizada en multitud de leyes, en el caso que nos ocupa puede significar la exclusión o no de determinadas situaciones y formas de acceso. Si se interpreta de una manera amplia incluiría tanto el acceso telemático mediante software como el acceso físico ya sea total o parcial.

Existen supuestos que a través de diferentes vías de acceso podrían concurrir en la infracción penal. El acceso remoto a otro equipo conectado en una red pública mediante una vulnerabilidad, acceder a un teléfono móvil salvando todas las medidas biométricas y claves desbloqueándolo o el acceso a un equipo informático de una compañía el cual se encuentra en un área reservada a pesar de que no haya medidas físicas de seguridad para acceder a tal.

Fernandez Teruel [10] comenta que se trata de un delito de medios indeterminados, en el que lo relevante es el resultado, asumiendo la posibilidad de que se utilicen todo tipo de fórmulas, tanto físicas como virtuales (directas o remotas); así, el acceso físico directo al sistema en el propio ordenador de la víctima o el control remoto de éste u obtención de los datos mediante aplicaciones que así lo permitan.

Es importante conocer en qué nivel y con qué finalidad se ataca la integridad del sistema y su política de acceso ya que si este acceso no autorizado es informado de manera inmediata al titular del sistema no supone un daño al bien jurídico protegido. En el momento que exista una afectación del sistema por mínima que sea, nos hallaremos ante una situación penable.

4.3 Diferencias entre el artículo 197 y 197 Bis.

Una vez analizados los distintos elementos del tipo, se pueden exponer de manera concreta las diferencias existentes entre el artículo 197 el artículo 197 Bis del Código Penal.

Si se enfoca con respecto a las medidas de seguridad, el artículo 197 no requiere de una protección mediante las mismas de manera que cualquier acceso es ilegal aunque no existan medidas de seguridad. El artículo 197 Bis no obstante, sí que exige que existan medidas de seguridad para la protección del sistema.

[10] Fernández Teruelo, J.G., Derecho e internet. Lex Nova, Valladolid 2011. Pág. 199.

Aunque en este sentido el artículo 197 pudiera parecer menos exigente que el artículo 197 Bis ya que además exige que se vulnere la intimidad, se revelen secretos accediendo a datos personales o familiares.

De manera contraria, el artículo 197 Bis no exige que se acceda a la información de carácter personal, pero si la vulneración del sistema y su privacidad, que ha de ser a través de la violación de las medidas de seguridad del mismo.

5. EL DELITO DE LA INTERCEPTACION DE DATOS.

Existen afirmaciones de que la LO 1/2015 ha introducido este delito en el apartado 2 del art. 197 Bis en una ubicación que no es la más idónea dado la falta de relación con el resto de apartados del artículo. Se podría fundamentar en la identidad del bien jurídico protegido, pero hay mucha diferencia en la conducta típica como para que sea regulado en el mismo artículo. Se expone que la ubicación más idónea hubiera sido un artículo 197 Ter.

El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

5.1 La interceptación mediante herramientas técnicas.

El acto de interceptar comunicaciones sin el consentimiento del otro usuario comprende el comportamiento típico cuando se realice mediante instrumentos técnicos.

La escucha, el seguimiento y el análisis de las comunicaciones deben ser incluidas además de la obtención de datos en la acepción de “interceptar”. De esta manera se puede afirmar que la observación de la comunicación, la captura y la grabación de los datos están englobados en este comportamiento. Según el Informe explicativo del Convenio de Budapest, incluye grabar, escuchar, monitorear o vigilar el contenido de las comunicaciones y tomar los contenidos de datos.

En el informe explicativo del Convenio de Budapest se destaca que con el requisito de la utilización de instrumentos o artificios técnicos se pretende limitar el acto ilícito solo aquellos comportamientos que se realicen a través del uso de dispositivos conectados a líneas de transmisión o intercepten comunicaciones inalámbricas. Aparte es, que para conseguir esto puedan realizarlo a través del uso de equipos físicos, software, códigos…

Finalmente, y como se extrae del propio texto ha de ser una interpretación no autorizada de la comunicación, de esta manera es totalmente aplicable el primer apartado del artículo 197 Bis del Código Penal.

5.2 El objeto material: las transmisiones de datos.

Como el objeto material son determinadas transmisiones de datos, estas también han de cumplir con una serie de requisitos.

Aunque no sea equiparable con que sean privadas, las comunicaciones no deben ser públicas, pero han de tener medias de protección al menos en la parte que se ataca. Si fueran comunicaciones privadas entre personas, se integrarían en el derecho a la intimidad, pero como ya se estimó antes, no es el bien jurídico protegido en este caso. De esta manera, la comunicación puede incluir información accesible al público pero con partes protegidas bajo medidas de seguridad. Un ejemplo de esto puede ser el pago por visión, ya que la información permanece protegida hasta que se efectúa el pago y queda liberada la información. de esta manera las comunicaciones que se realizan a través de la red pública no están excluidas tampoco.

Se requieren al menos unas mínimas medidas de seguridad, ya que hay tipos de comunicaciones que quedan excluidas de estos supuestos al carecer de ellas, un ejemplo claro de esto, podría ser las comunicaciones mediante walkie talki.

Otro requisito que según el Convenio se debe cumplir, es que las transmisiones deben ser automáticas, aunque este requisito es de interpretación ya que el texto no concluye nada al respecto. En la modificación de la LO 1/2015 si afirma que su objeto son las comunicaciones automáticas, que no personales, entre equipos.

Las transmisiones han de proceder del interior de un sistema de información. Las transmisiones pueden ser entre equipos, equipos e impresoras, equipos y personas, etc. Para no excluir ningún supuesto, en la legislación española se han incluido todo tipo de transmisiones para evitar las dudas a la interpretación.

Además de las transmisiones de datos, las emisiones electromagnéticas del equipo también están incluidas. Aunque no se especifica mucho en nuestra legislación, las emisiones electromagnéticas son ondas que desprenden los equipos y que debidamente tratadas pueden resultar en la reconstrucción de datos con la consiguiente revelación de información. Velasco Núñez[11] hace referencia a las mismas indicando que son emisiones o transmisiones entre sistemas, diálogos entre máquinas, no humanas, transmisiones automáticas entre equipos, máquinas, cuyos rastros y datos pueden dar información sobre costumbres privadas de un usuario, por ejemplo, si hay conexión con un router o si se está con un aparato encendido, que pueden dar información locativa o temporal sobre las costumbres de una persona.

De esta manera se puede concluir que solo será penable la interceptación de emisiones que por sí misma permita la reconstrucción de los datos o a través de la cual se puedan obtener directamente los mismos.

[11] VELASCO NÚÑEZ, E., Los delitos informáticos, Cuadernos Digitales de Formación 33-2015, Consejo General del Poder Judicial, pág. 23.

6. EL HACKING COMO DELITO CONTRA LA INTIMIDAD.

Al plantear el tema del bien jurídico protegido en base a las conductas antes mencionadas, este queda condicionado por el enfoque ante problemas tales como la exigencia de una finalidad jurídica o no a la simple curiosidad o el deseo de demostrar los conocimientos y destrezas que pueda tener un hacker.

A continuación, se va a intentar aclarar si el delito de hacking está incluido en los delitos contra la intimidad, la inviolabilidad del domicilio y el derecho a la propia imagen, una vez atendida la llamada función sistemática que cumple el bien jurídico protegido. Para esto se ha de considerar la localización sistemática del artículo 197 bis 1 del Código Penal.

El citado artículo se encuentra en el Titulo X del libro II del Código Penal, en concreto en su Capítulo I, el cual se refiere al "Descubrimiento y revelación de secretos". Así pues, el citado artículo se encuentra en la misma ubicación que el artículo al que actualizó, el artículo 197.3, introducido con la LO 5/2010.

Se ha de atender si la intimidad es el objeto del delito o por el contrario no lo es. Para ello conviene realizar una comparativa con los delitos más comunes históricamente contra la intimidad.

6.1 Acercamiento al bien jurídico común en los delitos contra el derecho a la intimidad.

El derecho a la intimidad es uno de los derechos fundamentales de nuestra constitución, más concretamente está recogido en el artículo 18. De esta manera, se puede afirmar que posee todas las garantías constitucionales de estos derechos.

En los siguientes apartados se expondrán las numerosas críticas que se han generado con la ubicación del delito de hacking entre los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, sobre todo por entender que con las reformas tanto de 2010 y 2015 o se tutela la intimidad de manera necesaria.

Según el esquema de Núñez Castaño [12], se puede unificar esta organización sistemática del derecho a la intimidad en el Código Penal de la siguiente manera:

- Acceso ilícito o no permitido a la intimidad, incluyendo los artículos 197 y 198, y que tras la reforma de la LO 1/2015, se incorporan los artículos 197 bis, 197 ter, 197 quarter y 197 quinquies
- Revelación de secretos por el obligado a guardarlos, que abarca su artículo 199
- Acceso no autorizado a datos de personas jurídicas previsto en su artículo 200
- Condición para la perseguibilidad de estos delitos en el artículo 201

[12] NUÑEZ CASTAÑO, E. *Nociones Fundamentales de Derecho Penal*, ed. Tecnos. Madrid, 2010, p. 225.

Con esta regulación de conductas en el Título X, se intenta proteger la intimidad frente a intromisiones de los demás en la vida privada de una persona en el ámbito penal, así como el habeas data, el secreto y derecho a la propia imagen. En el artículo 197 del Código Penal la intimidad individual es el bien jurídico protegido, por lo que las acciones ilícitas han de ser contra documentos, datos, sonidos o imágenes que sean importantes para salvaguardar la intimidad.

6.2 El hacking tomado como delito contra la intimidad.

En esta nueva era, se hace necesario plantear si con el delito de hacking, la intimidad, comprendida en el orden social actual con las nuevas tecnologías y las relaciones de los humanos con los sistemas informáticos, constituye el bien jurídico protegido.

Con la última modificación de 2015, el legislador ha decidido regular el hacking en un ámbito propio, pero sin desvincularlo de los delitos contra la intimidad ya que se mantiene en el mismo capítulo del Código Penal. Con esta modificación se produce una separación entre las conductas de acceso no autorizado y las conductas del descubrimiento o revelación de datos que atentan contra la intimidad personal.

6.2.1 Posturas negativas a la consideración del hacking como delito contra la intimidad.

El no considerar la intimidad como el bien jurídico protegido en el artículo 197 Bis del Código Penal, conlleva cierta controversia y no menos polémica dada su ubicación.

En esta corriente, fueron numerosas las críticas al ubicar el delito de hacking dentro del apartado 197 del Código Penal, en tanto en cuanto la realidad es que con este artículo se trata de preservar la privacidad del sistema informático más que la intimidad del usuario.

El artículo 197 Bis no ha aportado claridad para estos supuestos en torno al bien jurídico protegido con el delito de intrusismo informático, lo que ha hecho avivar más aún estas críticas, ya que en vez de separarlo de los delitos contra la intimidad lo ha mantenido en la misma ubicación.

Lo que en su día se consideró un acierto, como fue la reforma de 1995 para los delitos contra la intimidad ahora se han vuelto criticas ya que no solo se acoge al derecho contra la intimidad, sino también el derecho a la propia imagen y la inviolabilidad del domicilio. Se entiende que no existe criterio al añadir el delito de hacking con la reforma de 2010 ya que se contradice con el bien jurídico protegido que se estableció en 1995. De esta manera al ubicarlo en el artículo 197 del Código Penal se ha conseguido llegar a tener problemas de interpretación.

Toda esta controversia y este error se hubiera evitado si se hubiera creado un capítulo específico para este delito de acceso ilícito, ya que se identificarían de manera clara los bienes jurídicos protegidos y se eliminarían los problemas interpretativos. Con la última reforma de 2015 se piensa que el legislador ha dejado pasar otra oportunidad para mejorar el texto, y la ubicación en cuanto a los delitos contra la intimidad.

Donde sí se considera un acierto o al menos un mal menor es que con el acceso no autorizado a un sistema informático se entienda que se puede tener acceso a

información personal y se pueda afectar la intimidad, al menos se ha separado el delito de hacking de las conductas del artículo 197 del Código Penal, creando el 197 Bis en lugar del anterior 197.3 a pesar de no crear un capítulo o apartado propio.

Otra de las críticas que recibe, es que, si el bien jurídico protegido fuera la intimidad, los accesos no autorizados a sistemas informáticos públicos quedarían fuera de estas conductas. Así, si la intimidad fuera el bien jurídico protegido en el artículo 197 Bis del Código Penal, se plantearían problemas de delimitación en el momento que pudiera pensarse que los datos o software deben albergar información personal y dejarían fuera las conductas que se pretenden tutelar. Se puede poner de ejemplo en este caso el acceso no autorizado a sistemas informáticos de la administración pública, que si bien no tienen información privada o familiar sí que puede recoger cualquier otro tipo de información importante.

La jurisprudencia ha manifestado la importancia de la protección de la intimidad en la regulación de los acceso ilícitos a los sistemas informáticos, más allá de que los datos que contenga dicho sistema puedan considerarse irrelevantes o puedan detallar una configuración detallada del titular, afectando así a su intimidad, a lo que hay que añadir la emisión, recepción y almacenamiento de correos electrónicos en los sistemas, que conllevan el derecho al secreto en las comunicaciones, lo que conlleva como resultado la necesidad de protección frente a las conductas de hacking. Debido a esto, tanto desde el punto de vista de las garantías constitucionales que se exigen como desde el derecho de exclusión del propio sistema, la intervención de un equipo para acceder a su contenido exige un acto habilitante.

También, teniendo en cuenta la dificultad que supone determinar que actos, datos, imágenes o demás elementos pertenecen a la intimidad, Anarte Borrallo y Doval [13]País afirman que la interpretación de las nuevas conductas dentro del ámbito de la intimidad enmarca numerosos problemas, entre los que se pueden destacar varios.

- Sus elementos no se refieren expresamente a la intimidad.
- Si se considera como bien jurídico la seguridad de los sistemas de información, supone un adelantamiento de la intervención penal.
- En las normas comunitarias se descarta la intimidad como un bien jurídico protegido.

Da la impresión que se ha intentado enmascarar estas carencias no regulando los nuevos delitos en un lugar propio en el Código Penal y esto puede conllevar cierta incongruencia en los tribunales ya que los preceptos están ubicados entre los delitos contra la intimidad, y se tengan que aplicar por ejemplo a casos con intereses mercantiles.

Todo ello nos lleva a plantearnos si el nuevo delito de hacking debería haberse ubicado en un nuevo título del Código Penal junto a otros delitos relacionados con la informática como el delito de daños informáticos introducido en el artículo 264 del Código Penal tras la reforma de la LO 5/2010, obstaculizar o interrumpir el funcionamiento de sistemas informáticos previsto en el artículo 264 bis, producir, adquirir, importar o facilitar programas para cometer esos delitos, previsto en el artículo 264 ter, o cuando es una persona jurídica quien comete estos delitos, previsto en el artículo 264 quater.

[13] ANARTE BORRALLO, E. y DOVAL PAIS, A. "Delitos contra la intimidad ...", pp. 497 y 498.

La mayoría de autores coinciden en que la separación entre los delitos contra la intimidad y los delitos de acceso no autorizado a un sistema informático, tipificado en un título propio y autónomo, facilitaría la interpretación de los mismos y daría mejor solución en su afección a otros hipotéticos delitos.

7. LOS DELITOS INFORMATICOS EN EL AMBITO EUROPEO.

Prácticamente en todo el ámbito de las legislaciones penales europeas tienen en común que su punto de partida es el citado Convenio Europeo sobre cibercriminalidad, en cuyos artículos 2 a 6 se imponía a los Estados miembros la obligación de regular en el ámbito penal los "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos".

Como consecuencia de esta normativa europea, a fecha del presente trabajo han sido numerosos los países que han incluido en su legislación penal las conductas de intrusismo informático. Así ha sucedido con los países de nuestro entorno en el ámbito de la Unión europea, es decir, actualmente, Austria (1995), Bélgica (1958), Bulgaria (2007), Chipre (2004), Croacia (2013), República Checa (2004), Dinamarca (1973), Estonia (2004), Finlandia (1995), Francia (1958), Alemania (1958), Grecia (1981), Hungría (2004), Irlanda (1973), Italia (1958), Letonia (2004), Lituania (2004), Luxemburgo (1958), Malta (2004), Países Bajos (1958), Polonia (2004), Portugal (1986), Rumanía (2007), Eslovaquia (2004), Eslovenia (2004), Suecia (1995) y Reino Unido (1973)[14].

Sin embargo, a pesar de compartir el marco normativo europeo, la regulación del delito de hacking no ha sido igual en todos los casos, pudiendo clasificarse en los siguientes grupos:

- Los países que regulan en normas penales especiales los delitos informáticos.
- Los que tipifican el hacking en un título o capítulo propio y diferenciado dentro de su Código Penal.
- Los países que, como España, regulan el intrusismo informático junto a otros delitos, es decir, los restantes Estados citados.

Una vez presentada esta clasificación, se procederá a exponer brevemente a continuación las mencionadas legislaciones europeas con sus correspondientes particularidades.

7.1 Países que regulan los delitos informáticos en normas penales especiales.

Entre las legislaciones europeas donde se ha optado por regular el hacking de forma diferenciada de otros delitos, incluyéndolo en normas penales especiales, se encuentran las de Chipre, Portugal y Reino Unido.

7.2 Países que regulan el delito de hacking en un título o capítulo propio y diferenciado.

Las legislaciones de los países europeos que han optado por dotar de cierta autonomía a los delitos de hacking.

[14] Los países de la Unión Europea y el año de ingreso en la UE que se indica entre paréntesis están disponibles en http://europa.eu/about-eu/countries/index_es.htm, consultado 3 de abril de 2019.

Sin llegar hasta el punto de tipificar estos delitos en la legislación penal especial como en los casos mencionados en el epígrafe anterior, se regula el intrusismo informático en un título, capítulo o sección propia del Código Penal, de forma independiente a otros delitos. Así pues, en este apartado se citan los supuestos de Bélgica, Bulgaria, Croacia, Finlandia y Hungría.

7.3 Países que regulan el delito de hacking junto a otros delitos.

Se incluye la normativa de los Estados europeos que, como España, han optado por tipificar el delito de hacking junto a otros delitos que tutelan bienes jurídicos diversos a los de estas conductas.

Dentro de este grupo se encuentran la mayoría de países de nuestro entorno. En concreto, Alemania, Austria, Dinamarca, Eslovaquia, Eslovenia, Estonia, Francia, Grecia, Holanda, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Polonia, República Checa, Rumanía y Suecia.

7.4 Situación General.

La mayoría de las legislaciones de los Estados miembros de la UE no son lo suficientemente minuciosas en materia de hacking, limitándose a regular el tipo básico, ni tampoco dotan a estas conductas de la debida autonomía respecto a otras, con los consiguientes problemas interpretativos en cuanto al bien jurídico al que deben proteger y que parecen tutelar los instrumentos europeos que inspiran la citada normativa.

Así, aunque hay naciones que realizan una admirable y extensa regulación del acceso a los sistemas informáticos y sus variantes (Croacia, Finlandia, Hungría, Malta, Portugal y Reino Unido), también es cierto que la mayoría de legislaciones europeas optan por tipificar el intrusismo informático junto a los delitos contra la intimidad (Alemania, Austria, Grecia y Polonia), entre los delitos contra el honor y otros derechos individuales (Dinamarca), contra la propiedad (Eslovaquia, Eslovenia, Estonia, Francia, Malta, República Checa y Luxemburgo), contra el orden público (Holanda), junto a otros delitos de daños (Irlanda), contra la inviolabilidad del domicilio (Italia), contra la libertad y la paz (Suecia), o contra la seguridad (Letonia, Lituania y Rumanía), y todos ellos plantean los problemas de delimitación del bien jurídico protegido con los citados delitos.

Frente a esos casos mayoritarios, se encuentran los países que han decidido regular sistemáticamente los delitos informáticos (Chipre, Portugal y Reino Unido) o, al menos, por dotarles de cierta autonomía en un título o capítulo propio y diferenciado (Bélgica, Bulgaria, Croacia, Finlandia o Hungría).

Tras esto resulta que son muy pocos los países que tipifican detalladamente el hacking y, además, lo hacen de forma sistemática y separada de otros delitos que no están relacionados con estas conductas. En concreto, los citados casos de Croacia, Finlandia, Hungría, Portugal y Reino Unido. Además, entre ellos, es destacable que Hungría y Portugal ya regulasen esos supuestos incluso antes de ratificar en el año 2003 el Convenio Europeo sobre Cibercriminalidad.

Estos últimos casos demuestran que es posible una regulación ordenada de estos nuevos delitos, donde se incluyan unas definiciones de los conceptos esenciales, la

regulación del tipo básico y sus modalidades y todo ello en una sola norma, título o capítulo propio, que no plantee la amalgama de artículos, remisiones y bienes jurídicos afectados que encuentra el intérprete del actual artículo 197 Bis 1 Código Penal.

8. CASO DE EJEMPLO.

En el siguiente apartado se va a exponer un supuesto el cual podría estar recogido por el artículo 197 Bis del Código Penal. En este caso se tratará un acceso ilícito a un sistema que almacena información personal.

Una persona está segura de que desde hace un tiempo algunos documentos que almacena en su equipo personal y el contenido de algunos mensajes dirigidos de manera confidencial a otros destinatarios concretos han sido interceptados por terceros en la red. Sospecha que alguien ha accedido de manera ilícita a su ordenador y ha accedido a su información privada.

Este caso se podría encuadrar como un delito contra la privacidad. Los delitos contra la privacidad están recogidos en el artículo 197 y posteriores cuando se tratan de delitos informáticos en el Código Penal. Se los cataloga como delitos de descubrimiento y revelación de secretos, los cuales están dentro del capítulo de delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.

Según la legislación vigente, gracias a estos artículos se recogen tres conductas ilícitas básicas relacionadas con los sistemas informáticos. Primero la intercepción de comunicaciones sin permiso. Segundo, el acceso no autorizado a sistemas informáticos. Tercero, la vulneración de la intimidad del usuario a través de datos personales o familiares. Estas son las conductas recogidas como delitos informáticos contra la intimidad.

En el artículo 197.1 se comprende los delitos de apoderamiento de información. dicho artículo castiga las acciones realizadas para acceder a la intimidad de otra persona sin autorización a través del apoderamiento de emails, cartas, papeles o cualquier documento personal. Se puede afirmar que la legislación vigente no se termina de ajustar del todo a la situación actual ya que los comportamientos de espionaje informáticos, cuyas técnicas permiten acceder a un equipo ajeno revisarlo y sacar información sin tocar un papel no exige un desplazamiento o posesión física como se puede llegar a entender con este término de apoderamiento.

El actual artículo 197 Bis del Código Penal recoge el acceso no autorizado a un sistema informático sin producir más daños que el de la vulneración de las medidas de seguridad para su acceso.

8.1 Delitos de acceso no autorizado a un sistema informático.

Este tipo de delito sería el tipo que se expone en el supuesto. El hacker o pirata informático, desempeña conductas tales como los accesos no autorizados o interferencias de comunicaciones no autorizadas a un sistema informático o una red de comunicaciones. También se pena el mantenimiento o uso dentro de la red o el sistema.

Los comportamientos del hacker suelen ser de manera común únicamente eliminar los logs de conexión con el fin de borrar su rastro y evitar así ser identificados. Para ello, antes estudian la presencia de agujeros y fallos en las medidas de seguridad de los sistemas informáticos. De manera general, se entiende que el hacker posee conocimientos informáticos avanzados en cuanto al conocimiento de lenguajes informáticos y protocolos de internet.

8.2 Sentencias contra el acceso no autorizado a Sistemas informáticos.

Existen multitud de sentencias que recogen el acceso no autorizado a un sistema informático como una infracción penal. A continuación se citarán alguna de ellas.

"No sería aventurado adelantar que desde el punto de vista sociológico y en terminología anglosajona utilizada en, el ámbito informático las conductas que han sido descritas son las propias de un "hacker" o persona que utiliza determinadas técnicas para acceder sin la debida autorización a sistemas informáticos Buenos, o dicho en castellano, nos encontraríamos ante un intruso, figura diferente a la del "cracker" o pirata virtual que de manera intencionada se dedica a eliminar o borrar ficheros, a romper los sistemas informáticos y a introducir virus. La conducta del hacker está guiada por un deseo de vencer el reto intelectual de saltar las barreras del sistema. Tratan de vencer a las claves informáticas de los accesos, de descubrir, en suma, las lagunas de la protección. Por ello no es de extrañar que muchas compañías los contraten para que, antes de instalar sus sistemas informáticos, analicen si estos presentan grietas por las que se pude alguien colar en ellas". Su éxito presupone que se hayan burlado los medios de seguridad (contraseñas, claves de acceso, paswords), que están ahí colocados para impedirlo y que ponen de manifiesto la voluntad del titular de que la información que se contiene en los mismos no sea conocida más que por quienes están autorizados a ello».[15]

Como se expresó en el anterior apartado los comportamientos típicos del hacker comprenden el buscar y utilizar los defectos de las medidas de seguridad del sistema, bien sea a través de agujeros o puertas falsas o bien utilizando otro tipo de herramientas con el fin de acceder sin ser detectado. Según la legislación vigente, aunque no tenga otra finalidad más que el acceso, es decir, no esté interesado en la información que se guarda en el sistema, solo el acceso ya supone un acto ilícito más allá de la vulneración de la intimidad informática.

El acceso no autorizado comprende dos conductas que son punibles de cara a la legislación actual. Primeramente el acceso no autorizado a un sistema informático rompiendo o saltándose las medidas de seguridad del mismo, ya sea un sistema integrado por uno o más equipos.

La segunda conducta que puede ser penalizada por la legislación radica en el mantenimiento no autorizado dentro del sistema informático aun habiendo accedo de manera legítima al mismo. Si el infractor en cuestión continúa accediendo al sistema después de haberse revocado su autorización, se estaría cayendo en un acto de permanencia no autorizada más que de acceso no autorizado, aunque semánticamente encaje más la acción en la primera de las conductas.

De esta manera, en el caso que se está exponiendo en este apartado, se constituiría un acto de acceso no autorizado al equipo de la víctima, por lo que se podría denunciar ante la policía aportando todas las pruebas posibles que se pudieran sobre ello.

Una vez que se tramite la denuncia, se debe realizar un volcado de la información del sistema informático que pueda ser afectada por parte los agentes policiales

[15] Sentencia del Juzgado de lo Penal núm. 2 de Badajoz, de 15 de febrero de 2006

especializados en delitos de este tipo los cuales realizarán una impresión de estos datos y lo remitirán al juzgado correspondiente.

Sobre este volcado, la policía ha de identificar las conexiones realizadas de manera no autorizada y cotejar con los proveedores del servicio de internet a través de un requerimiento judicial esta información. una vez con esta información en su poder, la policía podrá identificar los equipos o terminales empleados en la intrusión y empezar la investigación propia de estos delitos siguiendo la metodología establecida.

Para que todo este procedimiento tenga lugar, se debe saber que tal y como se manifiesta en el artículo 201, “para proceder por los delitos previstos en este Capítulo será necesaria denuncia de la persona agraviada o de su representante legal” asique, en el caso de no realizar esta denuncia, este caso no podría ser perseguido a no ser que el caso cayera en lo que la propia ley catalogara como excepción.

A veces, es común que los atacantes con el fin de eludir su responsabilidad penal en el acto cometido, manifiesten que sus terminales fueron robados y no han sido ellos los que cometieron el acto. Por lo general, estas afirmaciones carecen de denuncia, y una vez que se realizan la policía acaba descubriendo que este alegato no es cierto.

8.3 Conclusiones sobre el caso.

En el caso que nos ocupa el mayor problema está en el acceso no autorizado a la información que se almacena en el equipo. En un momento dado se podría afirmar que, si el equipo es compartido, tal acceso serio licito si se realiza por una persona autorizada. En el momento en que se realice la revelación de secretos o de información privada de otro usuario se podría tipificar dentro del artículo 197 Bis, aunque Fermin Morales nos indica este problema.

“El tipo del artículo 197.3 (ahora 197 bis) expresa que el acceso debe verificarse sin autorización. Esta expresión abarca tanto los supuestos en los que el acceso se produce sin autorización del titular del sistema informático en el que se contiene los datos o programas como los supuestos en los cuales el acceso se produce con infracción de algún precepto legal que limita tal conducta. Por tanto, se trata de accesos ilícitos bien por falta de autorización del titular del sistema, bien por falta de autorización legal. No debe olvidarse que el nuevo precepto tipifica el acceso ilícito con vulneración de las medidas de seguridad establecidas para impedirlo, por tanto se tratará de conductas que reclaman una insiosidad, por cuanto ya se ha manifestado una voluntad de no autorizar un acceso abierto o libre al sistema.”

La segunda opción radica también en un supuesto recogido en el artículo sobre el que trata el trabajo que es el de la permanencia ilícita dentro del sistema informático sin tener autorización o en contra de la voluntad del titular. En este sentido se caería en el delito de allanamiento de morada y contra la intimidad. Esto vendría a decir que el domicilia informático es el espacio donde el usuario tendría la facultad de excluir y admitir a terceros a su conveniencia.

Por lo general se suele asociar que primeramente se ha de dar un acceso ilícito y posteriormente una permanencia en el sistema informático también de manera ilícita. Uno de los problemas radicara en si la juez vera necesario considerar que debe haber una vulneración de las medidas de seguridad del sistema informático o no para tipificarlo.

9. GRADO DE CONSIDERACION DE LA SOCIEDAD CONTRA LA CIBERDELINCUENCIA.

En la sociedad actual, siempre en movimiento y evolución, la ciberseguridad no puede ser una tarea o preocupación de quien se dedique a ello, debe ser algo compartido por todos. Se debe exigir un esfuerzo tanto a nivel organizativo como social.

En los últimos tiempos, el tener una cooperación directa y coordinada en materias de ciberseguridad se ha convertido en una necesidad que se ha visto reforzada debido los casos de ciberespionaje entre naciones. Casos como la acusación a principios de octubre del 2018 contra el gobierno ruso por una serie de ciberataques son prueba de ello. También se ha revelado que una operación conjunta de Holanda y el Reino Unido consiguió abortar un ciberataque ruso contra la Organización para la Prevención de las Armas Químicas.

Hoy día, hasta el más mínimo detalle puede ser importante a la hora de evitar posibles deficiencias en el sistema de seguridad de un equipo, y una acción pequeña puede tener un gran impacto a la hora de lograr una correcta protección del equipo.

Según Panda Security, se pueden describir diez medidas sencillas que pueden ayudar tanto a usuarios particulares como a compañías a mantener una correcta protección en sus equipos y sistemas informáticos

- Se ha de cambiar siempre las contraseñas predeterminadas, creando contraseñas sólidas y únicas para cada una de las cuentas y cambiarlas al menos una vez al año para mantener segura la información personal o privada.
- Utilizar la autenticación multifactorial siempre que sea posible, además de contraseñas seguras, para confirmar la identidad del usuario al iniciar sesión en sus cuentas.
- Utilizar un cortafuegos para bloquear el acceso no autorizado a equipos y dispositivos.
- Actualizar el sistema operativo, navegador y demás software con parches de seguridad para minimizar las amenazas de virus y malware.
- Limitar lo que se hace a través de Wi-Fi público y utilizar software que cree una conexión segura a través de Internet, como una Red Privada Virtual (VPN), para conectarse de forma segura desde cualquier lugar.
- Practicar la navegación y las compras de forma segura, comprobando que la dirección del sitio comienza con “https”, en lugar de sólo “http”.
- Habilitar la configuración de privacidad y aumentar la configuración de seguridad predeterminada del software que se utiliza.
- Ser selectivo cuando se comparta información personal, ya que esto podría ser utilizado por los hackers para adivinar contraseñas e inicios de sesión.
- No descargar software pirata, ya que no sólo es ilegal, sino que casi siempre incluye algún tipo de malware.
- Realizar una copia de seguridad de los datos, ya sea en un disco duro externo o en la nube, ya que es la forma más fácil de recuperarse de un ataque de ransomware.

En la actualidad, se espera que el número de ciberataques aumenten tanto en cantidad, como frecuencia y complejidad en tiempos venideros. Las compañías firmantes del Acuerdo sobre Tecnología y Ciberseguridad comparten la opinión de que

Internet es un recurso de uso compartido y por lo tanto su seguridad debe ser también compartida. Si todos los usuarios de la red emprenden acciones de manera colectiva con el fin de mejorar su entorno informático, la sociedad digital en la que vivimos se hará más segura, fuerte y resistente a futuros ataques.

Para poder definir los principios de la conciencia en ciberseguridad que debe tener nuestra sociedad, se ha de tener también en valor lo que supone la propia conciencia. Jose Antonio Marina Torres [16] hace una definición que se transcribe a continuación ya que se puede extrapolar al ámbito que ocupa el presente trabajo.

La palabra «conciencia» tiene dos significados. El primero, darse cuenta o percatarse de algo. En nuestro caso, de la importancia, dificultades, complejidades que tiene la seguridad y defensa de una nación. El segundo significado equivale a «conciencia moral», y hace referencia a los deberes, responsabilidades y al modo de cumplirlos. Una persona dormida, anestesiada o en coma no tiene conciencia en el primer sentido. Un criminal, un psicópata, no tiene conciencia en el segundo. Hago esta reflexión lingüística porque en el caso de la «conciencia de defensa» hay que utilizar ambos significados. Se trata de conocer la importancia, las dificultades, los problemas que plantea, y, también, la responsabilidad personal, ciudadana, ética y política.

Para el ámbito de conciencia nacional de seguridad cibernética es necesario utilizar ambas acepciones ya que es de vital necesidad ser conscientes de las amenazas y también es necesario conocer los deberes como usuario, miembro de una compañía o demás organismos; se ha de ser consciente de las responsabilidades que se han de tener tanto de manera individual como colectiva en el ámbito de la ciberseguridad. Tal y como se explica en la anterior definición, estas responsabilidades deben ser, personales, ciudadanas, éticas y políticas.

Para que la conciencia en ciberseguridad sea nacional y no presente carencias ni deje opciones a posibles atacantes ha de incluir tanto a ciudadanos, como compañías e instituciones.

Hoy día, el cibercrimen alcanza prácticamente a toda la ciudadanía en sus efectos, por lo que es necesarios cubrir todos los aspectos necesarios en los sistemas informáticos en lo que a seguridad se refiere con el fin de mantener la privacidad del usuario.

A pesar de que la informática está plenamente instalada en la sociedad y la navegación o comunicación a través de la red se ha vuelto incluso necesaria en el día a día, el concepto de ciberseguridad es relativamente novedoso, por lo que proporcionalmente no se encuentra gran cantidad de literatura sobre este tema.

9.1 Principios en los que se debe basar la conciencia social de ciberseguridad.

Ya en el principio del capítulo se detallan algunos consejos para ayudar a aumentar la seguridad de los equipos informáticos tanto a nivel particular como de organizaciones,

[16] MARINA TORRES JA, LÓPEZ MORA F, CONDE DE ARJONA F, MARRERO ROCHA I Y MORÉU MUNÁIZ F, Cuaderno de Estrategia n.º 155 del Instituto Español de Estudios Estratégicos, La Cultura de Seguridad y Defensa, un proyecto en marcha, Cap 2, pp 68.

pero se pueden también establecer una seria de principios con el fin de aumentar la conciencia de la ciberseguridad a nivel social.

- Se deben conocer las amenazas y los riesgos y se han de asumir.
- Se han de notificar los errores cometidos y se han de notificar también las incidencias de las que se ha sido víctima.
- Se ha de obtener información por parte de los responsables de seguridad de los sistemas informáticos de los ISP a los clientes o compañías a los que proveen.
- Se ha de formar a toda la sociedad. Se podría hacer por niveles según el nivel que corresponda a la necesidad de cada uno.
- Se ha de tener conciencia de adaptación al continuo cambio que sufren las circunstancias en el ciberespacio por parte de usuarios, instituciones y compañías.

A continuación se puede ver en una imagen que representa un edificio, los pilares sobre los que se sustenta la ciberseguridad a nivel de conciencia ciudadana.

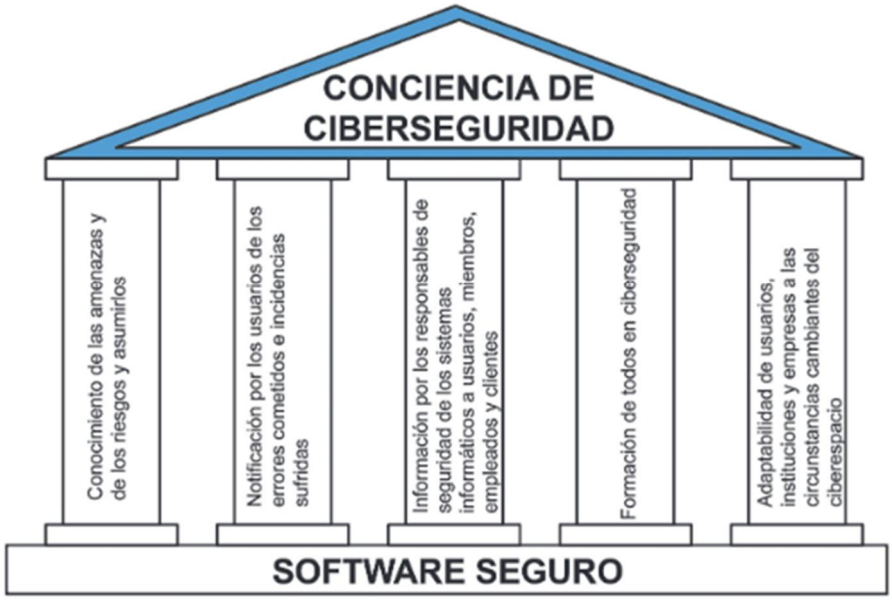

Ilustración 2Edificio de la conciencia de ciberseguridad.

Para que las posibilidades de éxito de los ataques se reduzcan, todas las personas que de una manera u otra hagan uso del ciberespacio han de ser conscientes de las amenazas que hay en el mismo y los riesgos indirectos que estas conllevan, de esta forma, los administradores y titulares de los sistemas informáticos, las compañías, los programadores, usuarios, etc. Podrán actuar cada uno en su ámbito.

En lo que se refiere a conciencia informática o en el ciberespacio, se refiere a hacer un uso responsable de éste.

Actualmente los niveles de vida que maneja la sociedad van directamente ligados al ciberespacio, sería imposible mantenerlos o mejorarlos sin su uso. La red eléctrica, gas o agua, su abastecimiento hoy día dependen de la informática. Incluso el disponer de nuestro dinero de manera instantánea sin llevarlo encima físicamente es posible gracias al ciberespacio y la informática.

De igual manera que es necesario realizar un uso responsable del ciberespacio, el uso irresponsable del mismo puede llevarnos a dejar de disponer de los servicios básicos incluso. Un uso irresponsable, no tiene que por qué ser un uso delictivo, puede ser tan solo un uso negligente, posiblemente por desconocimiento al no tener el antivirus actualizado o incluso el sistema operativo configurado de manera incorrecta, por citar algunos ejemplos.

Se sabe que el ataque con el virus Stuxnet a las centrifugadoras de la planta iraní de Natanz se hizo mediante de una pendrive que, de manera supuesta, llego accidentalmente a manos de uno de los ingenieros que trabajaban en la planta y que lo usó bien directamente en un equipo de control de la planta o bien en otro equipo en el que trabajaba en el software del sistema de control de la planta para luego copiarlo, junto con el virus, al sistema de control de la planta. El uso responsable del ciberespacio implica que antes de usar una memoria USB que llega casualmente al usuario, hay que comprobar qué tiene y cómo se comporta y, antes de usarla en un ordenador de la compañía pedir a los responsables de seguridad informática de la misma, si los hay, que la testeen; después, si no se está completamente seguro de que no tiene ningún malware, mejor no hacer uso de ella.

Se ha de tener claro que debido a la constante evolución de este ámbito nunca se llegara a ser totalmente inmune a los ciberataques, pero si es posible que se puedan abortar muchos intentas de accesos ilícitos y apropiación o modificación de material importante.

9.2 Formación de todos, cada uno en el nivel que corresponda, en ciberseguridad.

Hay un punto que es referente en este apartado, toda la sociedad ha de tomar conciencia en materias de ciberseguridad; formando desde la escuela, de jóvenes a mayores, pasando por empresas privadas y administraciones públicas, empleados y desempleados, etc.

No se trata de formar hackers, sino de que todos los ciudadanos tengan unas mínimas nociones de cómo mantener su entorno cibernético seguro, de qué y cómo se puede publicar en el ciberespacio sin comprometer la confidencialidad, privacidad y disponibilidad de los datos que se publican. Así mismo, hay que enseñar a toda la sociedad a utilizar las herramientas básicas de ciberseguridad como pueden ser antivirus, configuración del firewall y actualizaciones automáticas del sistema operativo.

Anteriormente a la instauración del Plan de Bolonia, es curioso que se puede comprobar que solo había como mucho una única asignatura que trataba el tema de la seguridad informática, y esta era optativa o de libre configuración en el último curso de la ingeniería informática, telecomunicaciones y demás derivadas. Actualmente las asignaturas no pasan de tres, de esta manera es difícil que los propios profesionales salgan correctamente formados en este tema y mucho menos concienciados. Esto redundara posiblemente en que no sean capaces de transmitir la idea de concienciación y de que tampoco sean capaces de crear sistemas que sean seguros.

En el campo de la formación profesional, se encuentra el mismo problema en el área de informática, solo existe una titulación de grado medio y otra de grado superior, y estas tienen una única asignatura de ciberseguridad.

En la actual situación, hay que empezar por formar y concienciar a los docentes en todos los niveles para que estos a su vez puedan formar a sus alumnos. Dependiendo del nivel y del área, esta formación variará. Dependiendo del nivel y del área, esta formación variará; en la mayor parte de los casos se trata solo de enseñar buenas prácticas en el uso de sistemas informáticos y de comunicaciones. Estas buenas prácticas no dejan de ser una especie de buena educación informática que podríamos llamar ciberurbanidad o cibereducación.

La concienciación pasa por mostrar el valor que tiene la información, los datos propios el daño que se puede llegar a sufrir tanto el usuario como el grupo al que pudiera pertenecer si se hiciera un uso erróneo de esa información, datos personales o demás información importante que estuviera en el sistema informático. Unos docentes concienciados en materias de ciberseguridad y con la ciberurbanidad asimiladas son muy importantes para implantar una conciencia de ciberseguridad basada en estos principios en personas en estado de formación.

Este planteamiento tiene su objetivo en el medio y largo plazo, pero es imprescindible para que las generaciones venideras interioricen estos principios se conciencien.

El ciudadano posee carencias en el conocimiento de amenazas y riesgos que ha de evitar con el uso de las nuevas tecnologías y esto se debe a diferentes factores. El principal es como ya se ha comentado, la gran velocidad de evolución que tiene el ciberespacio y lo relativamente poco que lleva y a la gran velocidad que se ha integrado en nuestra sociedad. Esta velocidad y si constante cambio, hacen de su complejidad otro de los factores.

La conciencia de ciberseguridad se ha de ir alcanzando de manera paulatina y según la persona hasta un grado y otro, pues no todas han de alcanzar el mismo. A esto, se ha de sumar la edad del individuo, pues también influye para alcanzar la conciencia en ciberseguridad, ya que su grado de madurez es sumamente importante. Se pueden establecer cuatro grandes grupos, que conformarían los grados de concienciación que se podrían alcanzar y distinguir entre la población.

El grado primero se podría llamar *ciberhigiene*. Es el grado básico y procura un nivel elemental de seguridad que, sin embargo, permite hacer frente a una elevada cantidad de amenazas. Básicamente son medidas que debe adoptar el usuario con el fin de prevenir ataques y amenazas y en su defecto, disminuyendo sus consecuencias. Principalmente son costumbres, que se han de asimilar y ejecutarlas de una manera automatizada pro parte del usuario. Estos automatismos son los que serán la base para el siguiente grado de concienciación.

Ciberconciencia podría ser el nombre del segundo grado, ya que es donde interviene la conciencia de la persona. Este grado es el que permite hacer un uso inteligente y responsable del ciberespacio y los recursos que se posean. Al contrario que los automatismos, en la conciencia si toma importancia el nivel de conocimiento que se pueda tener en un campo y la percepción que se obtiene del mismo. La creación de ciberconciencia requiere aprendizaje y experimentación, obteniendo los conocimientos necesarios para desenvolverse en el ciberespacio y extraer de forma segura el mayor provecho de sus posibilidades.

Una vez adquirida la ciberconciencia, esta se puede socializar, es decir, llegaríamos al tercer grado de concienciación al que se llamara *ciberciudadania*. Un ciberdciudadano es aquel que ejerce de manera coherente los derechos y deberes que corresponde al

usuario como ciudadano digital. Este grado tiene un mayor nivel de seguridad, ya que transciende de lo individual, apoyándose en el poder del grupo organizado mediante reglas.

Por último, se llegaría al ciberespecialista, el cuarto y último grado. Este cuarto grado supera al segundo en cuanto a conocimientos y preparación, tanto técnica como de otro tipo. Dentro de este grado se pueden establecer diferentes escalafones según los conocimientos que se posean. Estos son los usuarios que pueden realizar una aportación activa a la seguridad del ciberespacio. Sobre estas personas ha de recaer la responsabilidad de concienciar al resto de ciudadanos y combatir mediante estrategias y procedimientos de seguridad las posibles amenazas que puedan surgir.

9.3 Medidas de seguridad a tomar.

El objeto es sobre lo que se debe crear conciencia. Para ello, se utilizará del análisis efectuado el anterior apartado, desde el punto de vista de los riesgos. De este modo, a continuación, se trazarán las líneas generales sobre las que se debe actuar. En algunos casos se pueden dar una serie de solapamientos, pero ello resulta necesario para dar coherencia a cada misión.

- Protección física de los equipos y dispositivos. Por si mismo ya tienen valor y a la vez almacenan los datos e información del usuario.
- Protección de los datos personales. Es el objetivo del artículo que se trata en el trabajo, se debe tratar de mantenerlos de manera lo más segura posible. Esto pasa por hacer una transmisión responsable de los mismos, crear copias de seguridad así como tomar precauciones cuando se utilizan fuentes externas para almacenarlas.
- Protección en el acceso a nuestros dispositivos y sistemas mediante el uso de buenas prácticas en el mantenimiento y utilización de contraseñas.
- Protección de redes tanto físicas como inalámbricas con el fin de prevenir la intrusión.
- Lucha contra el malware, cerrando las vías de acceso y buenas prácticas en el uso de cortafuegos, antivirus y antispyware. Tenido también los programas actualizados, así como manteniendo una correcta configuración de los equipos y programas.
- Precaución en la navegación por Internet, con los archivos que se descargan y las compras que se efectúan.
- Apoyo a los menores frente a ataques específicos. Informar y crear espacios de confianza, así como mecanismos para ayudar a detectar, informar y combatir estos ataques.
- Respeto a las personas en el ciberespacio. Prevenirse contra Conductas ofensivas. Robo de identidad y ciberacoso.
- Respeto a la propiedad intelectual y datos ajenos. Descargas. Acceso a datos de los demás.

9.4 Métodos para lograr la concienciación social.

Ayudar a la concienciación social en materia de ciberseguridad es la finalidad que se busca en este trabajo tras analizar también la legislación vigente. Para esto se propondrán tres vías básicas para lograr el objetivo las cuales son la educación, la enseñanza y la concienciación.

Como se ha comentado el primer pilar básico será la educación. La educación es responsabilidad básica de los padres, que la comparten con los docentes cuando envían a sus hijos a la escuela. Hogar y escuela son, por tanto, los escenarios en los que se impartirá la educación. El objetivo es crear actitudes y valores en la persona e infundir buenos hábitos. Es aquí donde se conseguirá el adecuado grado de ciberhigiene, necesario para subir a los siguientes niveles. Al final de la educación, si se consigue el objetivo, se tendrá un adulto joven con un grado de conciencia que le permitirá desenvolverse como ciudadano digital.

La educación debe adaptarse a la edad de la persona y empezar de manera temprana. La manera ideal es practicarla con el ejemplo en la vida cotidiana, por esto, es básico, que tanto padres como docentes tenga concienciación en ciberseguridad y los conocimientos necesarios para aconsejar al menor en el uso de las tecnologías. El control parental se hace imprescindible hoy día para evitar riesgos y amenazas en el uso de aparatos tecnológico y en las transmisiones de datos.

Otra de las maneras de crear concienciación desde edades tempranas es la enseñanza. Desde la escuela se deben proporcionar conocimientos y habilidades. Que la persona aproveche sus recursos y se anticipe a las amenazas es la finalidad que se persigue. A través de la enseñanza se refuerzas los valores y actitudes inculcados en la educación, también en algunos casos además de complementar, debe compensar posibles deficiencias en la educación. Gracias a la enseñan a se puede alcanzar el grado de conciencia digital, es decir, el grado siguiente a la ciberhigiene. Una correcta armonización de enseñanza y educación plantean un escenario favorable para el desarrollo de la ciudadanía digital.

La enseñanza como camino para el desarrollo de la conciencia digital debe ser generalizada, no debe acotarse solo a asignaturas de contenido tecnológicos y se impartan preferentemente conocimientos técnicos. El uso de las TIC debe abarcar todas las materias siendo totalmente necesario en las escuelas. Se necesita continuidad en la vida académica del alumnado, mostrando además de teóricamente, ejemplo del bueno de las tecnologías. Son los profesionales de la enseñanza los que deben detectar que personas son aquellas que tienen cualidades para llegar a ser un ciberespecialista.

La concienciación sería el último camino a través del cual se pretende hacer que las personas sean sensibles a una situación, y a través de su conciencian, cambien sus actos y comportamientos en pos de una correcta actuación. Este nivel se ha de desarrollar en todos los estamentos de la sociedad. La concienciación asimila lo aprendido tanto en el hogar y la escuela y se adapta por sus propios medios a ellos. Este grado debe estar en evolución continúa debido a que la evolución del ciberespacio y sus amenazas presenta una evolución constante. La concienciación es fundamental para reducir las brechas digitales que tiene la sociedad; regionales, generacionales, sociales, económicas…

La concienciación debe encuadrarse en una estrategia concreta de seguridad a nivel nacional que defina objetivos, prioridades, coordinación y los medios necesarios para

llegar a conseguirla. Esta estrategia debe involucrar tanto al sector privado como al público, siendo liderada por el gobierno. Todo esto ha de ser complementado por un uso de las técnicas de información completo y veraz, de no ser así, se podría caer en una sensación de falsa seguridad y desconocimiento o también de una alarma generalizada de manera injusta.

En resumen, la concienciación digital deberá utilizar técnicas similares a las que ya se utilizan en otras campañas en las que se pretende abrir los ojos de la sociedad como puede ser la seguridad vial por ejemplo. Se han de utilizar todos los canales de comunicación posibles y darle continuidad a la campaña a lo largo del tiempo, ya que como se ha indicado anteriormente, tratamos sobre un ámbito muy cambiante.

Las administraciones públicas y demás estamentos deben completar las acciones de concienciación. Servicios como los CERT, publicaciones, páginas web o herramientas de seguridad gratuitas pueden aportar beneficios al resto de ciudadanos. De esta manera se reforzarían las campañas de concienciación y estas ganarían en credibilidad a la vez que se contribuye a mejorar la ciberseguridad.

Si se analiza detenidamente, los medios necesarios para fomentar la concienciación digital y ciberseguridad de la ciudadanía no suponen unos gastos elevados. Tiene mayor importancia el papel del poder político a través de la administración pública definiendo la estrategia y acciones a seguir en un plan de ciberseguridad general y del resto de actores para cooperar a fomentar esta concienciación. La creación de conciencia es un proceso paulatino que necesita tiempo y planificación. También resulta imprescindible adaptarse continuamente a la evolución de las amenazas.

10. LA CONCIENCIACION DE LAS COMPAÑIAS ANTE EL CIBERCRIMEN.

El ciberespacio se ha convertido en un recurso vital para la sociedad y su desarrollo gracias al gran desarrollo que han experimentado las TIC. Esto es, gracias a que facilita y favorece la relación entre los usuarios y las administraciones públicas y empresas. Su creciente importancia ha despertado el interés de numerosas organizaciones como la OCDE, Organización para la Cooperación y el Desarrollo Económico que señala internet como un "*elemento fundamental para impulsar el desarrollo económico y el bienestar social, así como para fortalecer la capacidad de las sociedades para mejorar la calidad de vida de sus ciudadanos*".

Como cabe esperar todo no puede ser beneficioso, y toda ventaja alberga su lado menos satisfactorio y este radica en que la dependencia de las redes es cada vez más elevada, esto además conlleva que el nivel de exposición ante riesgos y amenazas es cada vez más elevado también. La relevancia que han tomado las redes de comunicación ha llevado a la necesidad de aumentar su protección ante cualquier tipo de incidentes que las puedan alterar, ya que su caída o modificación podría afectar de manera muy grave a funciones sociales de gran importancia.

A nivel internacional esto ha quedado plasmado en que se han planteado diversas estrategias de ciberseguridad, habiendo multitud de países que han creado sus propios documentos como son Estados Unidos, Reino Unido, Francia, Canadá, Alemania, Japón y Holanda. Así, por ejemplo, en la Estrategia de Ciberseguridad del Reino Unido[17], ya se afirmaba que "*el coste medio de un incidente de seguridad de la información para una PYME era de entre 10.000 y 20.000 libras y para una gran empresa, con más de 500 empleados, podía llegar a ser de entre un millón y dos millones*".

De esta manera, es manifiesta la importancia que para las compañías supone tener un buen desarrollo en políticas y conocimientos en ciberseguridad. De esta manera, teniendo una concienciación desarrollada de su papel en el ciberespacio podrá ser consciente de las amenazas y riesgo que tienen para su normal actividad en la red.

Las buenas prácticas de seguridad son una serie de rutinas implementadas con el fin de salvaguardar la integridad de la compañía y evitar en la medida de lo posible que sea víctima de ataques o accesos no deseados.

10.1 Buenas prácticas de seguridad para las compañías en la red.

En el siguiente apartado se darán una serie de pautas o buenas prácticas para las empresas que trabajen en el ciberespacio con la finalidad de aconsejar o concienciar en pos de que se mantenga integra en el mismo tanto a nivel de datos como de accesos.

[17] Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space, junio de 2009.

10.1.1 Uso de Certificados.

El despliegue de productos TIC ha de ser una de las buenas prácticas básicas a desarrollar por una compañía, estos productos deben haber sido certificados por entidades independientes. Que una compañía utilice productos certificados supone un mayor nivel de seguridad para la organización ya que éstos han sido evaluados previamente por terceros. Que estén certificadas supone que estas herramientas han sido probadas y declaradas libres de vulnerabilidades en ese momento.

Actualmente existe un esquema global, llamado norma Common Criteria que siguen la mayoría de las entidades certificadoras. Estas pueden ser propietarias o bien estar especializadas en algún ámbito. A continuación se detallará tal norma.

La norma “Common Criteria” recoge los criterios comunes como su propio nombre indica para la evaluación de los productos TIC. Constituye un estándar internacional que establece criterios comunes, rigurosos y objetivos para dicha evaluación de seguridad.

Esta norma está formada por una serie de documentos que tratan los diferentes aspectos que se deben de tener en cuenta en la evaluación de un producto TIC, es decir, todo el software y firmware o hardware acompañado por sus respectivas guías de instalación y uso que estén dentro del alcance de dicha evaluación.

Esta norma no es específica para ninguna tecnología en concreto y puede ser aplicada para evaluar la seguridad de cualquier producto TIC. Esta norma esta completada por unos criterios de evaluación, CEM, los cuales son aplicados por todos los laboratorios acreditados para realizar estas certificaciones.

Cabe destacar que Common Criteria, CC y Common Methodology for IT Evaluation, CEM, han sido reconocidos como estándares internacionales, conformando las normas ISO/IEC15408 e ISO/IEC18045, respectivamente.

10.1.2 Consumo de productos Certificados CC.

Si la compañía en cuestión se decidiera a realizar las buenas prácticas que aconsejan el uso de productos certificados, debe seguir una serie de pautas para elegir el más idóneo.

La manera más adecuada para valorar la idoneidad de un producto certificado es a través de un análisis de riesgos para la organización en el que se puedan cotejar las amenazas que se desean mitigar, para poder así elegir los productos que más se ajusten a las necesidades de la compañía y que permitan mitigar el riesgo detectado.

Una compañía que vaya a adquirir algún producto certificado ha de valorar las propiedades de seguridad que ofrecen cada uno de los productos certificados seleccionables. Para esto debe basarse en las declaraciones de seguridad y en los informes de certificación pertenecientes a los productos y comparar a partir de ahí con el análisis previo de riesgos que se ha hecho por parte de la compañía.

10.2 Buenas prácticas para la gestión de la información.

En este apartado se expondrán las normas más ventajosas para la gestión de la seguridad de la información a través de buenas prácticas.

10.2.1 ISO 27000: Sistemas de gestión de la seguridad de la información.

Un sistema de gestión de la seguridad de la información, SGSI, es una herramienta que permite a una organización mantener el nivel de riesgo asociado al manejo de sistemas de información y comunicaciones por debajo del umbral establecido por sus titulares. Para de proporcionar un marco de referencia común para su desarrollo y basándose en experiencias previas en este ámbito, la ISO, Organización Internacional para la Normalización (International Organization for Standardization) ha elaborado un conjunto de normas, y las ha agrupado en la serie ISO 27000.

Esta nueva serie de normas creadas por ISO, recoge su experiencia en el desarrollo de otros sistemas de gestión a nivel corporativo, como pueden ser calidad o medioambiente. En todos sus modelos comparte la visión de orientar el sistema hacia una mejora continua, mediante el PDCA, Plan Do Check Act.

Las principales normas de la serie ISO 2700 son la ISO/IEC 27001 y la ISO/IEC 27002, ambas editadas por la Organización Internacional para la Normalización en 2005.

La norma ISO/IEC 27001:2005, es el documento básico de la serie 27000 y en él se especifican los requisitos mínimos que la organización debe cumplir para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de un Sistema Informático, definiendo las acciones a realizar en cada una de las fases del PDCA.

Por otro lado, la norma ISO/IEC 27002:2005, complementa a la primera, la ISO 27001 y, al contrario que esta, no es certificable. Su objetivo es proporcionar una relación de medidas de seguridad fruto de la experiencia acumulada en este ámbito y que pueden ser utilizadas como referencia a la hora de seleccionar las medidas de seguridad asociadas al establecimiento y mantenimiento de un Sistema de Gestión.

10.2.2 Controles críticos de Seguridad.

Los *20 Critical Security Controls* o *20 Controles críticos de seguridad para una ciberdefensa efectiva* son una serie de medidas de seguridad que tienen por objetivo servir como elemento de apoyo a la decisión, que proporciona una guía que permite a las organizaciones o compañías priorizar sus inversiones en materia de seguridad y garantiza que las medidas que se implantan son aquellas cuya efectividad ha quedado acreditada por la experiencia real. De esta manera, se persogue maximizar el retorno de la inversión realizada en la implantación de medidas de seguridad.

La NSA, National Security Agency o la Agencia de Seguridad Nacional de los Estados Unidos es donde radica el origen de estas mediad de seguridad. Actualmente el CCA o Consortium for Cybersecurity Action, un consorcio internacional, es quien se encarga de la revisión y el mantenimiento, en este consorcio se integran más de cien agencias y departamentos, compañías privadas y organismos públicos de Australia, Reino Unido y Estados Unidos.

De manera progresiva, la importancia de los 20 controles de seguridad se ha ido incrementando en los últimos años.

En su edición más reciente los 20 controles críticos son, en orden de importancia decreciente, los siguientes:

1. Inventario de dispositivos autorizados y no autorizados.
2. Inventario de software autorizado y no autorizado.
3. Configuración segura de hardware y software en dispositivos portátiles, estaciones de trabajo y servidores.
4. Evaluación y tratamiento continuos de las vulnerabilidades.
5. Protección contra el código malicioso.
6. Seguridad de las aplicaciones.
7. Control de dispositivos inalámbricos.
8. Capacidad para la recuperación de datos.
9. Evaluación de las capacidades relacionadas con la seguridad y formación apropiada.
10. Configuración segura de dispositivos de red: cortafuegos, routers y switches.
11. Limitación y control en el uso de puertos de red, protocolos y servicios.
12. Uso controlado de los privilegios de administración.
13. Defensa perimetral.
14. Mantenimiento, monitorización y análisis de ficheros de auditoría (logs).
15. Control de accesos basado en la necesidad de conocer.
16. Control y monitorización de cuentas.
17. Prevención de pérdida de datos.
18. Gestión de la respuesta a incidentes.
19. Ingeniería de red segura.
20. Pruebas de penetración y ejercicios Red Team

10.3 La concienciación sobre Ciberseguridad de las empresas.

Una vez expuestas alguna de las rutinas de buenas prácticas más relevantes a llevar a cabo por las compañías, se va a proceder también a exponer otra serie de rutinas que ayudarían a mejorar la concienciación dentro de la propia organización.

10.3.1 Programas de concienciación y formación.

Si se parte de la premisa que el factor humano suele ser el detonante de muchos errores y por ende el eslabón más débil de la cadena en cuanto a seguridad, hay que plantear como las compañías pueden difundir todos los conceptos analizados anteriormente para la seguridad así que todos los miembros de la misma tienen los conocimientos adecuados a su rol dentro de la organización.

Para esto, se debe analizar cómo se puede implantar un programa de concienciación de ciberseguridad como herramienta mediante la cual difundir el conocimiento sobre los riesgos para la ciberseguridad y las posibles medidas para combatirlos y así asegurar la consecución de los objetivos de concienciación citados anteriormente.

Como se explicó anteriormente, existen distintos niveles de aprendizaje según los roles y responsabilidades que se tengan dentro de la compañía, a continuación se desarrollaran brevemente ya que confluyen con los ya citados en anteriores apartados.

La *concienciación* es un proceso de aprendizaje destinado a todos los miembros de la compañía y está enfocado a modificar actitudes individuales y colectivas para comprender la importancia de la seguridad y las consecuencias que puede tener una mala praxis.

La pregunta a la que trata de responder es el cómo, ya que el objetivo que tiene es que el personal conozca que habilidades necesita para desempeñar un rol determinado.

Se pueden poner como ejemplos de canales para proporcionar este aprendizaje los vídeos, folletos, comunicados por email, posters, banners, etc. Se busca alcanzar un impacto en un corto espacio de tiempo.

La *educación* es el proceso de formación más avanzado y persigue el desarrollo de las capacidades y la visión para realizar actividades complejas y también promover el desarrollo profesional en ciberseguridad.

La pregunta a la que trata de responder es el por qué, ya que el objetivo que tiene es que el personal desarrolle una conciencia más profunda y sea capaz de gestionar su conocimiento en la materia.

Para obtener este tipo de aprendizaje se incluye el desarrollo y la investigación, seminarios y demás cursos que se puedan realizar. El impacto temporal que se busca alcanzar es a largo plazo.

Las acciones de concienciación han de centrarse en las funciones de trabajo específicas, o roles y responsabilidades de ciberseguridad, que desempeñen los trabajadores, no en los títulos de sus puestos de trabajo. De hecho, una persona puede tener más de una función en la empresa y, por tanto, necesitará capacitación en ciberseguridad para poder cumplir con las responsabilidades específicas de cada rol que desempeñe.

Como se puede comprobar, toda la organización necesita una formación básica en los conceptos y procedimientos de ciberseguridad. Superiormente a este nivel básico, en función de los roles y responsabilidades desempeñadas, se pueden establecer diferentes niveles de capacitación de ciberseguridad, como por ejemplo podrían ser principiantes, intermedios o avanzados.

Se debe analizar de manera cuidadosa por parte de la empresa los objetivos de concienciación de ciberseguridad que se van a realizar para asegurar así que se cubren todas las necesidades. Deben analizarse las necesidades específicas en ciberseguridad de un grupo determinado de roles más allá de la concienciación básica que necesita toda la compañía.

La *dirección ejecutiva*, las personas que dirigen la compañía han de conocer de manera completa la normativa y la legislación sobre ciberseguridad que sea de obligado cumplimiento dentro de su corporación. Adicionalmente, han de comprender su papel de liderazgo en lo que a ciberseguridad se refiere para así asegurar que la gente que este bajo su mando cumpla con la normativa vigente dentro de la organización.

El *personal de seguridad*, son las personas que actúan como consultores expertos dentro de la organización incluyendo a los directores de los programas de seguridad. Han de tener un gran conocimiento de la política, los procedimientos y las mejores prácticas de ciberseguridad.

Los *responsables funcionales* deben poseer un conocimiento amplio de la política de seguridad y un alto grado de comprensión de los requisitos de ciberseguridad que se puedan aplicar, según el tipo de información que manejen, así como de los controles de seguridad con los que puedan satisfacer dichos requisitos en los sistemas de información de su responsabilidad.

Los *administradores de sistemas y personal de soporte TI* son responsables de realizar las operaciones necesarias para una correcta implementación y funcionamiento de las medidas de seguridad a nivel técnico. Estas personas han de tener un alto nivel de conocimiento de las medidas implementadas tanto a nivel teórico como practico.

Los *usuarios*, son las personas que deben tener un alto grado de concienciación y formación en determinados controles técnicos de seguridad también en los procedimientos que utilizan para desarrollar sus actividades profesionales dentro de la compañía.

Queda patente tras lo expuesto que las compañías necesitan desarrollar los correspondientes programas de concienciación y formación en ciberseguridad para salvaguardar la integridad de todos los departamentos que la compongan. Estos programas se pueden desarrollar en las siguientes tres fases según el ENISA, Empresa Nacional de Innovación S.A.:

La primera fase seria *Planificar, estimar y diseñar*. Los programas de formación y concienciación han de ser diseñados teniendo siempre en cuenta la misión, visión y objetivos de cada compañía. Es muy importante que apoyen las necesidades de negocio y que influyan en la cultura de la empresa y, también, en las arquitecturas que soportan sus servicios TI. Los programas más exitosos son aquellos en los que los usuarios consideran que son relevantes para los problemas que se tratan de resolver.

En esta etapa se identifican las necesidades de formación y concienciación, se debe diseñar un plan eficaz que cubra las necesidades, se busca y se asegura la disponibilidad de los servicios de formación necesarios y se establecen las prioridades para llevarlas a cabo. En esta fase se deben llevar a cabo las siguientes actividades:

- Establecer el equipo inicial del programa de concienciación.
- Adoptar un enfoque de gestión del cambio que incluya una estrategia adecuada de comunicación.
- Definir objetivos y metas.
- Definir los grupos y audiencias objetivo.
- Identificar el material de formación y el personal necesario para impartir el programa.
- Evaluar las posibles soluciones, analizando la posibilidad de externalización o la impartición con medios propios de los cursos formativos.
- Seleccionar la solución y el procedimiento de impartición, identificando los beneficios del programa.
- Obtener el apoyo de la alta dirección y la financiación adecuada, por medio de una adecuada identificación de los costes que permita hacer un plan de negocio formal para validar y justificar la necesidad de las inversiones requeridas.
- Elaborar el plan de trabajo, que debe incluir la lista de actividades, los hitos y el calendario, así como la distribución de los recursos y el presupuesto por cada actividad.
- Desarrollar el programa y las listas de comprobación de las tareas.
- Definir el concepto de comunicación, incluyendo el plan de comunicación y los canales para llevarlo a cabo.
- Definir los indicadores para medir el éxito del programa, identificando los grupos de audiencia a los que se les va a aplicar los indicadores y definiendo las métricas a utilizar

- Establecer la línea base para la evaluación.
- Documentar las lecciones aprendidas.

La segunda fase sería la de *desarrollar y gestionar*. En esta fase se incluye cualquier actividad necesaria para implementar el programa de formación y concienciación sobre ciberseguridad. Las acciones del programa, que ejecuta la estrategia establecida para cubrir las necesidades de formación identificadas, solo se podrán gestionar y llevar a cabo una vez haya sido desarrollado el correspondiente material formativo.

En esta fase se deben llevar a cabo las siguientes actividades:

- Confirmar el equipo de trabajo del programa.
- Revisar el plan de trabajo.
- Iniciar la ejecución del programa.
- Entregar las comunicaciones.
- Documentar las lecciones aprendidas

La tercera y última fase para la creación del plan de concienciación sería la de *evaluar y ajustar*. Los mecanismos de evaluación son componentes críticos para cualquier programa de concienciación sobre la ciberseguridad. La mejora continua solo se logrará si podemos conocer cómo está funcionando el programa actual. Además, hay que tener en cuenta que los mecanismos de evaluación se deben diseñar para alcanzar objetivos establecidos inicialmente para el programa. Una vez que se han alcanzado los requisitos iniciales básicos de concienciación, se puede diseñar y comenzar a aplicar una estrategia de mejora continua.

En esta fase se deben llevar a cabo las siguientes actividades:

- Realizar evaluaciones que permitan medir el éxito del programa.
- Recopilar los datos, de forma automática y/o manual que permita analizarlos y obtener una retroalimentación.
- Incorporar la retroalimentación para futuros programas.
- Revisar los objetivos del programa.
- Poner en práctica las lecciones aprendidas.
- Ajustar el programa según sea necesario.
- Volver a iniciar el programa de concienciación.

11. RECOMENDACIONES DE LAS PRINCIPALES ORGANIZACIONES EN CIBERSEGURIDAD.

Actualmente existe un buen número de marcos de control y buenas prácticas sobre ciberseguridad que pueden ser de gran utilidad para que las organizaciones afronten este reto. Hacer uso de ellos hará más fácil la comprensión de los riesgos y amenazas que existen en la actualidad y facilitará la implantación de las medidas correctas a la realidad de la compañía.

Seguidamente, se muestran algunos de los ejemplos más significativos, incluyendo algunas de los organismos de referencia en el ámbito de la ciberseguridad, tanto a nivel nacional como internacional.

No hay que olvidar que el sector se encuentra en constante evolución, pudiendo surgir nuevas referencias. Es importante mantenerse activo en la búsqueda de soluciones y nuevas prácticas si se pretende luchar con éxito contra los riesgos asociados a la ciberseguridad.

Primeramente, se empezará mostrando las medidas que se toman a nivel nacional y a continuación se hará un breve desarrollo de las principales organizaciones mundiales en materia de ciberseguridad y las medidas que proponen y sus principales publicaciones.

11.1 INCIBE.

El Instituto Nacional de Ciberseguridad de España, INCIBE, llamado con anterioridad Instituto Nacional de Tecnologías de la Comunicación, INTECO, fundado en 2006. es una sociedad dependiente del Ministerio de Economía y Empresa a través de la Secretaría de Estado para el Avance Digital y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

INCIBE trabaja para afianzar la confianza digital, elevar la ciberseguridad y la resiliencia y contribuir al mercado digital de manera que se impulse el uso seguro del ciberespacio en España.

Su actividad se basa en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE contribuye a cimentar ciberseguridad a nivel nacional e internacional.

INCIBE es una herramienta del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para esto, con una actividad que se basa en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

INCIBE pone a disposición de toda la sociedad española una gran cantidad de recursos e información relacionada con la ciberseguridad.

Entre muchas otras utilidades, en su página web se puede encontrar un apartado específico denominado “Protege tu empresa”, y que incluye por ejemplo las siguientes guías:

- *Como gestionar una fuga de información.*
- *Gestión de riesgos.*
- *Ciberseguridad en comercio electrónico.*

Además, INCIBE, proporciona a los usuarios un catálogo completo de empresas que proveen soluciones de ciberseguridad, además de un servicio gratuito con el que conocer si su equipo está infectado.

Para la formación y concienciación cabe mencionar la actividad que desempeña la Oficina de Seguridad del internauta, www.osi.es, la cual tiene como objetivo prestar ayuda a los usuarios de internet a conseguir la adopción de buenos hábitos de seguridad, mediante la concienciación de la comunidad sobre los riesgos existentes y ayudando a reducir la cantidad y gravedad de los incidentes sufridos por los propios usuarios.

Los valores que promueve INCIBE son los siguientes:

- Transparencia con la sociedad en general y los agentes del ámbito de la ciberseguridad en particular.
- Búsqueda de la excelencia, tanto en la aptitud y en la actitud de sus profesionales, así como en la ejecución de los proyectos.
- Vocación de servicio público.
- Mantenimiento del espíritu innovador y de la búsqueda de la excelencia en los proyectos que se abordan, maximizando el valor ofrecido.
- Sostenibilidad como valor ético y criterio de desempeño que involucra los aspectos económicos, sociales y medioambientales de la actividad.
- Espíritu de integración, apoyo y cooperación con todos los agentes relevantes en ciberseguridad, reforzando las capacidades nacionales en seguridad.

11.1.1 Actividades de INCIBE.

INCIBE desarrolla numerosas actividades con el objetivo de aumentar la ciberseguridad nacional, pero se puede afirmar que se apoya en cuatro pilares fundamentales.

El instituto promueve *servicios* en el ámbito de la ciberseguridad que permitan la explotación de las TIC y aumenten la confianza digital. Precisamente, INCIBE trabaja en mecanismos para la prevención y reacción a incidentes de seguridad de la información, y promueve el desarrollo de la cultura de la seguridad de la información a través de la concienciación, la sensibilización y la formación.

El siguiente pilar básico es la *investigación*. INCIBE cuenta con una importante capacidad para abordar proyectos complejos de diversa naturaleza y con una fuerte mentalidad innovadora. INCIBE también cuenta con capacidad para generar inteligencia en ciberseguridad que confluya en la mejora de los servicios.

La *promoción y la detección de talento* también cobra vital importancia para INCIBE, esto favorece a que todos los sectores relacionados, sector académico, industria y

profesionales se sirvan de la oportunidad que la confianza digital da para la innovación, la generación de talento y la investigación avanzada, constituyendo así un mercado de productos y servicios competitivo y de referencia internacional.

El último pilar y no menos importante es la *coordinación*. INCIBE participa en redes de colaboración nacionales e internacionales que facilitan la inmediatez, globalidad y efectividad a la hora de desarrollar una actuación en el campo de la ciberseguridad, contando siempre con una perspectiva basada en la experiencia y en el intercambio de información.

INCIBE diseña y desarrolla sus soluciones para solventar las necesidades específicas de determinados grupos como pueden ser los siguientes.

Empresas y profesionales que hacen uso de las TIC. Las empresas y organizaciones disponen de apoyo preventivo y reactivo en materia de seguridad en tecnologías de la información y la comunicación para aprovechar de la mejor manera posible las posibilidades de las TIC de forma segura y confiable. Con una atención especial, INCIBE centra esfuerzos para la protección de los sectores estratégicos, imprescindibles para la economía y la sociedad, así como a las instituciones afiliadas a RedIRIS.

Expertos en ciberseguridad. INCIBE, a través de su equipo con personal especializado en ciberseguridad, brinda servicios de información y respuesta a colectivos y profesionales expertos para mejorar los niveles de ciberseguridad en España.

Ciudadanos. La Oficina de Seguridad del Internauta, OSI, anteriormente descrita, es el servicio gratuito que provee de información y soporte al usuario final para evadir y solucionar las incidencias de seguridad que le pueden surgir al navegar por Internet, esto suele pasar sobre todo, en los primeros pasos en las nuevas tecnologías.

Otro grupo lo forman los *menores, jóvenes, familias, educadores y profesionales del ámbito del menor*. Internet Segura for Kids (IS4K) es el Centro de Seguridad en Internet para menores de edad en España y tiene por objetivo el impulso del uso seguro y responsable de Internet y las nuevas tecnologías entre los niños y adolescentes. Forma parte de la red paneuropea INSAFE de Centros de Seguridad en Internet y está cofinanciado por la Comisión Europea.

Además de todo el desglose que se han presentado para el alcance, la concienciación y el servicio de ayuda, para acometer su labor, INCIBE cuenta con las siguientes capacidades:

Amplio ámbito de actuación en la respuesta a incidentes de seguridad abarcando desde el ciudadano hasta el sector empresarial (especialmente, a sectores estratégicos e infraestructuras críticas) y al ámbito específico de RedIRIS.

Puesta en marcha de iniciativas de colaboración público-privada para la mejora de los niveles de ciberseguridad en España.

Seguimiento y estudio de los riesgos emergentes para poder anticipar necesidades, adoptar medidas preventivas y, en definitiva, disponer de mecanismos de alerta temprana.

Coordinación con actores clave a nivel nacional e internacional en materia de ciberseguridad.

11.1.2 Kit de concienciación de INCIBE.

Los empleados de las compañías son los encargados de procesar, gestionar, modificar, eliminar, transmitir y almacenar la información en una empresa. Son el engranaje principal para el buen funcionamiento, por esta razón hay que plantearse si conocen los riesgos en materia de seguridad.

Puede haber riesgos por desconocimiento y desinformación que sitúen a una compañía en una situación crítica. Se puede formar a los empleados por medio de la concienciación en materia de Ciberseguridad.

En este sentido, INCIBE pone los medios a través de un programa: KIT de Concienciación, que incorpora múltiples recursos gráficos, elementos interactivos y una programación detallada.

En la siguiente imagen se pueden diferenciar los elementos que componen el Kit de Concienciación de INCIBE.

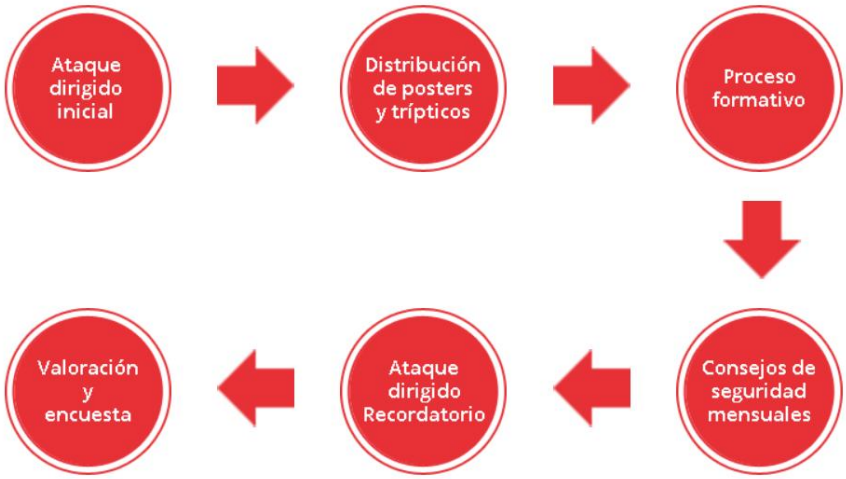

Ilustración 3 Kit de Concienciación. Fuente:INCIBE

A continuación se va a desarrollar cada uno de los elementos que componen el Kit de Concienciación según se explica en la propia web de INCIBE.

Manual de implantación

El manual es la guía de aplicación del kit, contiene información sobre los materiales además de una programación para su distribución dentro de una empresa.

Ataques dirigidos

La conciencia empieza con uno o dos ejercicios que van a permitir evaluar el nivel de concienciación en seguridad de nuestros empleados a la vez que despertamos su interés por aprender más. Estos ejercicios toman la forma de ataques sorpresa.

Se incluyen dos ataques dirigidos para ser lanzados, uno por correo electrónico y otro por medio de un pendrive USB. Pueden lanzarse ambos al comienzo o uno al comienzo y otro al final de la concienciación. En el manual se explica con detalle cómo lanzar estos ataques.

Pósteres y trípticos

Después de lanzar un ataque dirigido distribuiremos en lugares de paso frecuente dos tipos de materiales: pósteres y trípticos.

El kit incluye pósteres en dos tamaños (A3 y A2). Con estos elementos principalmente gráficos se pretende concienciar a los empleados para que se consideren una parte activa de la seguridad de nuestra empresa.

Además de los pósteres, se han realizado para este kit una serie de trípticos que podemos dejar a disposición de nuestros empleados. Los trípticos combinan gráficos y textos para transmitir aspectos importantes de seguridad relacionados con los cuatro bloques temáticos.

Proceso formativo

Una vez despertado el interés, se plantea realizar un proceso formativo combinando la distribución de material para su lectura y visualización con la opcional organización de charlas. Esta fase consta de cuatro bloques temáticos o píldoras: la información, los soportes, el puesto de trabajo y los dispositivos móviles.

Cada píldora está compuesta de los siguientes materiales: videos interactivos, presentaciones, documentos de texto, salvapantallas y test de autoevaluación.

Ilustración 4 Fuente:INCIBE

Para fomentar la participación de los empleados el kit dispone de cuatro videos interactivos asociados a las píldoras. En ellos se transmiten consejos y buenas prácticas en nuestro puesto de trabajo y entorno laboral. Representan escenas cotidianas en una oficina cualquiera. En las escenas hay iconos sobre los cuales se puede hacer clic para leer los distintos consejos.

El kit incluye a modo de refuerzo cuatro presentaciones, una para cada una de las unidades temáticas, que pueden ser utilizadas en una charla. Con ellas podemos repasar los conceptos claves y las medidas de seguridad básicas, así como buenas prácticas cuando se trabaja con información sensible. La información en ellas es concisa, ya que un documento de texto acompaña a cada una de ellas con la explicación detallada de los conceptos.

Cada una de las píldoras está explicada en un documento de texto. Estos documentos contienen información sobre los conceptos, medidas y buenas prácticas mencionadas en las presentaciones y los videos interactivos. Las presentaciones y los documentos pueden bien distribuirse para una lectura individual o explicarse por un orador en una sesión formativa.

Una vez se ha revisado el material anterior, se ofrecen imágenes con consejos o recordatorios para poner durante varios meses como salvapantallas o fondos de escritorio. Se han de cambiar cada mes para que se visualicen todos.

Finalmente unos test de autoevaluación con preguntas sobre cada temática permiten al usuario comprobar los conocimientos adquiridos.

Consejos de seguridad mensuales

A modo de resumen se incluyen unos ficheros con gráficos que contienen consejos temáticos para reforzar lo aprendido. Estos materiales se pueden enviar por correo, publicar en un blog interno o distribuirse de forma impresa.

Encuesta de satisfacción.

Una vez terminado el proceso de concienciación en la empresa se puede hacer llegar un feedback de la experiencia y opinión mediante la encuesta de satisfacción. Como ocurre en otros casos, la colaboración es muy importante para mejorar este kit.

11.2 CIS, Controles Críticos de Seguridad.

Los Controles Críticos de Seguridad, fueron creados en 2008 por el Centro de Seguridad de Internet, CIS. A través de una colaboración del gobierno de Estados Unidos y diversas organizaciones de investigación sobre seguridad del sector privado. Un conjunto de defensas prácticas concretamente dirigidas a contener los ciberataques, estas defensas planteadas eran de naturaleza técnica y tenían el propósito de definir etapas prácticas específicas que una organización podría tomar para evitar que las ciberamenazas más comunes comprometan sus sistemas de información.

Los controles CIS están diseñados para dar prioridad y enfoque, para aprovechar el poder de una gran comunidad de expertos para identificar y apoyar prácticas de gran valor y pasos esenciales, y para dejar de "contemplar el problema".

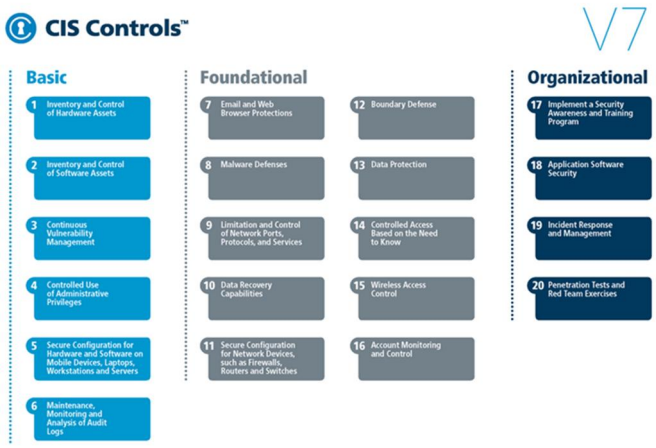

Ilustración 5controles CIS, fuente: www.cisecurity.org/controls/

Los controles CIS adoptan el principio Pareto 80/20, el principio de que tomar solo una pequeña porción de todas las medidas de seguridad que posiblemente se puedan

tomar, produce un porcentaje muy grande del beneficio de asumir todas esas acciones posibles.

Mientras que los Controles CIS se centran en la acción técnica, los desarrolladores de éstos afirmaron que muchas de estas recomendaciones obligarían a los equipos técnicos operacionales a modificar las rutinas para mejorar tanto los controles operacionales como la seguridad, replantear sus estrategias básicas de defensa y ser más estructurados y disciplinados en sus actividades. Por lo tanto, el éxito con los Controles de CIS (o cualquier programa defensivo) depende de que las compañías desarrollen y trabajen a partir de una nueva hoja de ruta integral para mejorar la ciberdefensa.

Cuando los Controles CIS son introducidos a algunas organizaciones, puede surgir el desánimo pensando que los Controles reflejan un objetivo demasiado alto inalcanzables por la compañía. La implementación exitosa de los controles requerirá que muchas organizaciones cambien su forma de pensar sobre la ciberseguridad y la forma en que afrontan las operaciones y la defensa de TI.

Los empleados ya no pueden instalar software por su cuenta o viajar con datos confidenciales en su poder. Se ha establecido que necesariamente la aceptación cultural de los cambios necesarios para implementar los controles técnicos es necesariamente requisito previo para el éxito. Este es probablemente el obstáculo más importante que la mayoría de las organizaciones deben superar. En este sentido, la compra y el refuerzo de la dirección ejecutiva son primordiales.

Numerosas organizaciones han tenido éxito en la implementación de los controles en un enfoque por etapas o fases, empezando por algunos controles y subcontroles primeramente e implementando otros de acuerdo con un plan coordinado y aprobado por la administración superior. Además, dividir el trabajo de implementación de los controles entre varios individuos / equipos también ha demostrado acelerar el progreso de la implementación. Es raro que las organizaciones implementen cada subcontrol descrito en los controles CIS (la versión 6.0, por ejemplo, tiene 149 subcontroles). Hay subcontroles que brindan asesoramiento sobre técnicas avanzadas mientras que la mayoría de los subcontroles son fundamentales para la ciberdefensa efectiva.

El estar continuamente revisando y actualizando su postura en ciberseguridad hace que la seguridad de las organizaciones sea más fuerte supervisando además las amenazas en evolución. En un promedio de entre uno y tres años, las organizaciones que implementan los Controles CIS deben asumir que sus esfuerzos tomarán para alcanzar así un nivel satisfactorio de conformidad con los controles CIS. Se debe empezar por los controles más críticos y apara instaurar la totalidad de los controles es posible que se tarde alrededor de cinco años de esfuerzo dedicado a ello. Según el nivel de las inversiones variara la velocidad de la implementación.

11.2.1 Implementación de los Controles Críticos.

Para lograr una mejor ciberhigiene, las organizaciones que estén considerando implementar los controles críticos han de planificarlo cuidadosamente. La creación de una estructura organizativa para los Controles CIS ayudara a alcanzar el éxito a la mayoría de las organizaciones. Un programa de GRC, Gobierno, Riesgo y Cumplimiento puede ser establecido por parte de algunas organizaciones. Otras tácticas exitosas incluyen asignar desarrolladores de software, administradores de programas para coordinar las tareas relacionadas con la implementación de controles CIS por

administradores de servidores, ingenieros de redes, especialistas en estaciones de trabajo e incluso profesionales externos a la tecnología de la información como especialistas en recursos humanos, capacitadores y demás roles importantes para el correcto funcionamiento de la estructura.

Para que les sirva como basa a otras normas o medidas de seguridad muchas organizaciones ya están implantando una estructura de seguridad. En muchas organizaciones, los regímenes de seguridad como el Framework de ciberseguridad NIST, la alineación del NIST y la serie ISO 27000 o las reglamentaciones como HIPAA, FISMA, PCI DSS, NERC CIP ya se están siendo utilizadas para definir los controles de ciberseguridad. Actuar según determinados estándares no es inconveniente para las organizaciones hagan uso de los Controles CIS, los cuales les ayudaran a alcanzar estándares adicionales. Actualmente hay definiciones de los Controles CIS prácticamente para todos los estándares de seguridad, ya que les ayudara a la correcta organización y la consecución de otros objetivos.

La implementación de los Controles CIS acarrea una seria de beneficios indirectos ya que la implementación de los controles de mayor prioridad, es decir los cinco primeros ayudaría a la compañía a lograr los beneficios más importantes. De tal manera, la implementación del inventario de activos (Controles CIS 1 y 2) y las configuraciones estándar (Control 3) a menudo da como resultado ahorros de costes generales para la compañía, ya que se requieren menos sistemas y administradores de red para administrar el entorno de ciberseguridad de la organización. El tamaño de la organización será proporcional al coste de la implementación de los controles. Si nos basamos en la economía de escala, las compañías con mayor tamaño gastaran más recursos generales en ciberdefensa, mientras que las compañías más pequeñas gastaran un mayor porcentaje de su presupuesto total en ello. El uso del ciberespacio como una herramienta de trabajo conlleva un coste asociado que es el de proteger a la organización de los ciberataques que pueda sufrir.

Hay una serie de sugerencias que se deben tener en cuenta a la hora de implantar los Controles CIS y que pueden ayudar a optimizar dicha implementación y conseguir el éxito en la misma. Para esto la organización debe:

- Hacer que los Controles CIS sean parte del estándar de defensa de la organización. La directiva debería estar involucrados para recibir apoyo y resultados.
- Asignar un administrador del programa, que deberá estar cualificado y será responsable de la implementación de los controles CIS.
- Decidir quién será responsable de la sostenibilidad a largo plazo del mantenimiento de las medidas de defensa.
- Comenzar con un análisis de amenazas, evaluación o auditoría del estado actual de la organización en los Controles CIS y desarrolla un plan de implementación programado con enfoque prioritario en los primeros cinco controles.
- Documentar el plan a largo plazo de implementación de defensas de ciberseguridad que no sean parte de la estrategia defensiva de la organización.
- Incluir las definiciones u objetivos de los Controles CIS en la documentación de la organización, creando políticas de seguridad para mejorar su implementación.

- Asegurar que los auditores internos y externos usan los controles CIS como parte de su punto de referencia para evaluar la estructura de seguridad de la organización.

Aunque puede haber múltiples sugerencias adicionales, las que se han mostrado en párrafos anteriores pueden suponer un punto de partida óptimo para comenzar la implementación de los controles CIS.

11.2.2 Los primeros 5 controles críticos.

Para lograr una correcta ciberhigiene es imprescindible tener implementados los cinco primeros controles de seguridad critica CIS, ya que diversos estudios afirman que con la implementación de estos controles ya se puede presentar una defensa eficaz ante los ataques más comunes, que suelen ser alrededor del 80% del total de los ataques. A continuación, se van a describir cómo se implementarán los cinco primeros controles CIS.

CSC 1 | Inventario de dispositivos autorizados y no autorizados.

El fin de este control es ayudar a las organizaciones a definir un total de lo que se debe defender. Sin una visión de qué dispositivos y datos están conectados, no pueden ser defendidos. Los escáneres (tanto activos como pasivos) colocados en la red de la organización que puedan detectar dispositivos puede ser un punto de partida. Este proceso de inventario debe ser tan completo como sea posible. Después de que una organización haya inventariado con precisión sus sistemas, el siguiente paso es evitar que los dispositivos no autorizados se unan a una red, aquí es donde cobra importancia el proceso de implementación de la autenticación a nivel de red. El objetivo inicial no es evitar que los atacantes se unan a la red, sino también comprender qué hay en la red para poder defenderla.

CSC 2 | Inventario de software autorizado y no autorizado.

El objetivo de este control es garantizar que solo se permite la ejecución de software autorizado en los sistemas de información de una compañía. Si bien un inventario de software es importante, el control más importante que una organización puede implementar aquí es la inclusión en la lista blanca de aplicaciones, que limita la capacidad de ejecutar aplicaciones solo a las que están explícitamente aprobadas. Este Control a menudo se considera uno de los más efectivos para prevenir y detectar ataques de ciberseguridad, aunque la lista blanca de aplicaciones a menudo no se implementa fácilmente. Este esfuerzo requerirá que una organización reconsidere sus modelos operativos ya que los usuarios ya no podrán instalar el software que deseen cuando y donde quieran. Pero este Control, ya implementado con éxito por numerosas organizaciones, probablemente proporcionará beneficios inmediatos a una organización que intenta prevenir y detectar ataques específicos en su contra.

CSC 3 | Configuraciones seguras de hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores.

En la mayoría de los sistemas, esta configuración va enfocada a la facilidad de uso y no al aumento de la seguridad. Los sistemas pueden tener la capacidad de ser protegidos, pero es probable que existan configuraciones que un sistema debe tener para garantizar una alta seguridad. La mayoría de las organizaciones ya cuentan con los sistemas de tecnología necesarios para configurar de manera segura sus sistemas

a escala. Los Objetos de directiva de grupo de Microsoft Active Directory y Unix Puppet o Chef ya están comúnmente establecidos en las organizaciones

CSC 4 | *Evaluación continua de la vulnerabilidad y remediación.*

El objetivo de este Control es comprender las debilidades técnicas del software que está instalado en los sistemas de información de una organización y eliminar o paliar esas debilidades. Las organizaciones con éxito implementan sistemas de administración de parches que cubren vulnerabilidades tanto de sistemas operativos como de aplicaciones de terceros, por lo que garantizan su correcta actualización en todo momento. Esto permite la instalación automática, continua y proactiva de las actualizaciones para abordar las vulnerabilidades del software.

CSC 5 | *Uso controlado de privilegios administrativos.*

El objetivo de este Control es garantizar que los miembros de la fuerza laboral solo tengan los derechos, privilegios y permisos del sistema que necesitan para realizar específicamente su trabajo, ni más ni menos de lo que establece su rol dentro de la organización. A veces, de manera desafortunada, por razones de velocidad y conveniencia, muchas organizaciones permiten que el personal tenga un sistema local o incluso derechos de administrador de dominio que son la puerta de entrada a ataques, accidentes o incidencias de otro tipo. La solución simple para este Control es eliminar permisos o permisos innecesarios del sistema de la organización. Actualmente, para las organizaciones de mayor tamaño que están intentando realizar esta tarea a gran escala, existen proveedores de administración de privilegios que pueden proporcionar soluciones de administración de puntos finales para ayudar a disminuir la carga administrativa.

11.3 NIST 02-2014.

El NIST o National Institute of Standards and Technology establece interesantes referencias y buenas prácticas a través de metodologías y normas, cuyo objetivo no es otro que el de promover la innovación y competitividad industrial para las organizaciones.

En de su gran creación de marcos de referencia, se puede destacar por su utilidad en el tema que se está tratando, la ciberseguridad el “Framework for Improving Cybersecurity”. Este documento, de carácter público y disponible a través de su web, muestra un enfoque basado en 25 riesgos para la gestión de la ciberseguridad y se compone de tres apartados, el marco base, los niveles y los perfiles. En el presente trabajo se expondrá el marco base ya que es donde se facilitará la información más relevante de cara al apartado que se está presentando.

Un *Marco Base*, que es un conjunto de actividades de cada a la correcta gestión de la ciberseguridad. Está dividido en 5 funciones que son identificar, proteger, detectar, responder y recuperar que, a su vez, se dividen en 20 categorías.

Ilustración 6Fuente: NIST

es posible que socios de negocio, clientes o incluso organizaciones gubernamentales requieran el cumplimiento del marco de trabajo dentro de sus consideraciones contractuales, aunque no se trata de una guía de implementación discrecional con base en las mejores prácticas y estándares de la industria.

Actualmente la implementación de este marco es asumible a nivel internacional de manera indistinta por cualquier organización de manera independiente a su tamaño, riesgo o nivel de sofisticación de sus medidas de seguridad a pesar de que en un principio esta fue desarrollada con respecto a la protección de infraestructura critica de Estados Unidos.

Este marco de trabajo no es un documento estático, cualquier compañía u organización puede adaptarlo a sus necesidades y determinar qué actividades considera prioritarias a la hora de la implementación permitiendo así un despliegue progresivo y personalizado.

En base a que la base del marco de trabajo está establecida en la integración de los criterios de diferentes estándares, directrices y mejores prácticas a nivel internacional, su implementación no está limitada únicamente a Estados Unidos. Así pues, su despliegue fuera de Estados Unidos agrega una nueva capa de cooperación e integración global en ciberseguridad, ya que este tema que no está restringido a un ámbito geográfico en particular.

11.4 SANS y CIS.

SANS, Audit, Networking and Security Institute es una reputada organización norteamericana de investigación y educación cooperativa que brinda recursos y noticias sobre seguridad. Entre sus artículos se puede destacar mucha información importante en materia de ciberseguridad. Dentro de sus recursos, se encuentra “Securing The Human”, que ofrece herramientas de concienciación gratuitas.

SANS es la organización de mayor tamaño en el Mundo de formación de seguridad en las TIC y la que posee mayor reputación. Sus cursos de seguridad son desarrollados por líderes de la industria en numerosos campos, incluyendo seguridad de red, auditoría, forense, liderazgo y seguridad de aplicaciones.

Intentando minimizar los robos de información que estaban sufriendo principalmente las organizaciones de defensa estadounidense principalmente, en 2008 se inició u proyecto con el fin de elaborar una guía sobre buenas prácticas en seguridad de la información. esta guía fue llamada “Critical Security Controls for Effective Cyber Defense”. En 2015 fue transferida al CIS de Estados Unidos.

Esta guía contiene un total de 20 acciones claves o controles críticos que las compañías deberían implementar con el objetivo de prevenir, detectar o paliar los ciberataques.

11.5 CESG UK GOV.

CESG, Communications Electronics Security Group, es la autoridad especializada en materia de seguridad de la información en Reino Unido.

Esta organización ha publicado numerosos artículos entre los que destaca “Ten Steps To Cyber Security”. Esta publicación es una guía que aconseja sobre como las organizaciones pueden protegerse en el ciberespacio mediante diez pasos o consejos. Inicialmente se publicó en 2012 aunque al igual que todos los elementos que rodean este ámbito ha sufrido varias evoluciones. En la guía se tratan como las 10 principales prioridades la gestión de los siguientes aspectos:

- Conexión Segura.
- Seguridad de la red.
- Modelo de información de los riesgos de ciberseguridad.
- Gestión de incidencias.
- Protección ante el malware.
- Control de dispositivos con riesgo de ser borrados.
- Monitorización de seguridad.
- Política de teletrabajo, tanto en el hogar como móvil.

11.6 ISACA.

ISACA, Information Systems Audit and Control Association, está presente en Desarrollo de buenas prácticas en auditoría y control de sistemas de la información. Ha publicado infinidad de documentos destinados a los profesionales entre los que cabe destacar la guía para la aplicación del marco NIST, mencionado en anteriores apartados, para la ciberseguridad, “Implementing the NIST Cybersecurity Framework”, dentro de su programa Nexus para la ciberseguridad creado tras la aprobación de la ley de ciberseguridad en Estados Unidos en 2015 con la finalidad de otorgar a los profesiones de la seguridad informática los conocimientos y herramientas necesarios para realizar correctamente su trabajo.

Además, dentro de la última revisión del CobiT, cuyas guías representan unos de los mejores ejemplos de buenas prácticas para los principales estándares en el ámbito del control y la supervisión de tecnología de la información a nivel mundial, ISACA ha ido actualizando su marco de trabajo para ir proporcionando una guía de practica de seguridad de la información de la empresa totalmente actualizada en todos sus niveles prácticos para así ayudar a las empresas a reducir sus perfiles de riesgo a través de una administración de seguridad adecuada.

11.7 ENISA.

La European Union Agency for Network and Information Security, ENISA ofrece en su página web intercambio de información, buenas prácticas y conocimiento en el ámbito de la ciberseguridad.

Un reglamento publicado en junio de 2013 encomendaba a ENISA el campo de actuación y la autoridad necesarios que les permite la lucha contra el ciberdelito:

- Desarrollo de políticas y legislación de la Unión Europea en materia de ciberseguridad.
- Investigación, desarrollo y estandarización de normativa.
- Prevención, detección y respuesta a ciberamenazas fronterizas.

Aunque sus recomendaciones están orientadas a estrategias nacionales de ciberseguridad, su lectura puede ayudar a extraer buenas prácticas aplicables a la realidad de las organizaciones.

11.7.1 Análisis de ENISA de la legislación actual.

En un nuevo informe la agencia de seguridad cibernética ENISA ha tomado una instantánea sobre la actual y futura legislación comunitaria en materia de medidas de seguridad y denuncia de incidentes. Este análisis pone presente importantes pasos hacia adelante y también identifica lagunas en la implementación nacional y expone que la mayoría de los incidentes no son reportados.

Los incidentes cibernéticos tienen un impacto significativo en la sociedad. He aquí cinco ejemplos bien conocidos del inicio de esta era:

- En 2012, millones de contraseñas de redes de negocios fueron expuestas
- En 2011, la tormenta Dagmar destruyó millones de enlaces de comunicación escandinavos
- En 2011, un fallo en un centro de datos británico interrumpió millones de comunicaciones empresariales en todo el mundo
- En 2011, una autoridad de certificación fue violada desvelando comunicaciones de millones de usuarios
- En 2010, un proveedor de telecomunicaciones chino pirateó el 15% del tráfico mundial de Internet durante 20 minutos.

En lo que llevamos de año algunos de los incidentes en cuanto a seguridad informática que hayan destacado pueden ser los siguientes.

- Spectre y Meltdown. Una serie de vulnerabilidades críticas en procesadores Intel y métodos de ataque de canal lateral que permitían saltarse el ASLR,

un mecanismo de protección incluido en los sistemas operativos basado en la aleatorización de ubicaciones de la memoria RAM haciendo disminuir así el rendimiento de la misma.

- Facebook comprometió la información personal de 30 millones de usuarios.
- La cadena de hoteles Marriott informó de una de las mayores violaciones de seguridad de la historia, con robo de datos personales y financieros de 500 millones de clientes.
- Google+ cerro después que un nuevo bug comprometiera la información de más de 52 millones de usuarios.

Se ha progresado mucho, un grupo de trabajo de ENISA para los reguladores nacionales ha desarrollado tanto un conjunto común de medidas de seguridad así como un formato de reporte de incidentes. ENISA suele recibir reportes e informes reguladores sobre grandes incidentes de seguridad informática. Este material se utiliza como recurso para la estrategia europea de seguridad cibernética European cyber security strategy y la European cyber security exercise. El director ejecutivo de ENISA, el profesor Udo Helmbrecht, comentó que "*El reporte de incidentes es esencial para obtener una imagen real de seguridad cibernética. La estrategia de seguridad cibernética de la UE es un paso importante y uno de sus objetivos es ampliar el alcance de la declaración de provisiones, más allá del sector de las telecomunicaciones*."

12.CONCLUSIONES.

Actualmente se viven momentos realmente interesantes para realizar reflexiones como las que se han llevado a cabo en este TFM. Cada vez hay más incidentes sobre ciberseguridad en los espacios informativos y se informativos y se considera, en las estrategias de seguridad de todos los países, incluida España, que la ciberseguridad es un elemento clave a tener en cuenta en tiempos venideros para el desarrollo de una sociedad civil formada de manera adecuada, de unas organizaciones con formación y tecnologías suficientes de prevención ante los incidentes derivados de la misma y de una Administración Pública dotada de tecnologías y formación para prestar al ciudadano los servicios públicos que se necesitan con garantías suficientes y que permita que la ciudadanía se relacione con la Administración de forma segura y confiable, avanzando, como en el caso de nuestro país, en el desarrollo de la agenda digital. Y parte fundamental de esta agenda digital es la ciberseguridad.

La mayoría de las legislaciones de los Estados miembros de la UE no son lo suficientemente minuciosas en materia de hacking, limitándose a regular el tipo básico, ni tampoco conceden a estas conductas de la necesaria autonomía respecto a otras, con los consiguientes problemas interpretativos en cuanto al bien jurídico al que se protege y que parecen tutelar los instrumentos europeos que inspiran la citada normativa en el que se basa el artículo base del trabajo, el artículo 197 Bis del CÓDIGO PENAL.

El artículo 197.3, relativo al acceso ilícito a los sistemas informáticos fue modificado por la LO 1/2015, como consecuencia de la Directiva 2013/40/UE, que traslada esas conductas al artículo 197 bis 1, incluyendo como novedad el castigo en la misma norma de las conductas de facilitar a otro el acceso y la referencia al hecho del acceso al sistema de información. Esto supone la sustitución de la anterior mención a datos o programas informáticos.

Así, aunque como se ha visto algunos países realizan una loable extensa regulación del acceso a los sistemas informáticos y sus variantes (Croacia, Finlandia, Hungría, Malta, Portugal y Reino Unido), también es cierto que la mayoría de legislaciones europeas optan por tipificar el intrusismo informático junto a los delitos contra la intimidad (Alemania, Austria, Grecia y Polonia), entre los delitos contra el honor y otros derechos individuales (Dinamarca), contra la propiedad (Eslovaquia, Eslovenia, Estonia, Francia, Malta, República Checa y Luxemburgo), contra el orden público (Holanda), junto a otros delitos de daños (Irlanda), contra la inviolabilidad del domicilio (Italia), contra la libertad y la paz (Suecia), o contra la seguridad (Letonia, Lituania y Rumanía), y todos ellos plantean los problemas de delimitación del bien jurídico protegido con los citados delitos.

La regulación de las conductas de hacking en la mayoría de los países de nuestro entorno europeo no es lo suficientemente meticulosa, limitándose a la regulación del tipo básico y omitiendo otros supuestos que pueden surgir en torno al intrusismo informático. Tampoco dotan a estas conductas de la debida autonomía respecto de otras, originando problemas interpretativos similares a los que acontecen en el Código Penal español.

Las naciones que tipifican sistemáticamente las conductas entre los delitos informáticos (Chipre, Irlanda, Portugal y Reino Unido) o, al menos, les otorgan cierta autonomía en un título o capítulo propio y diferenciado (Bélgica, Bulgaria, Croacia, Finlandia o Hungría) son minoría.

Se han formulado distintos conceptos del fenómeno hacking, distinguiendo el hacker blanco del cracker, que realiza el acceso para causar un daño al sistema o a su titular, phreackers, que utilizan los sistemas telefónicos para realizar interceptaciones sin ánimo de lucro, o los viruckers, cuya finalidad es introducir un virus en el sistema informático, de tal forma que el concepto gramatical identifica a los hackers como las personas que utilizan determinadas técnicas para el acceso sin autorización a un sistema informático ajeno, habiendo optado la mayoría de los países por no distinguir la finalidad del hacking, poniendo fin a la distinción del hacking blanco y sancionar todos los supuestos de acceso a los sistemas ajenos.

Así pues, desde el punto de vista normativo se identifica hacking con cracking, razón por la cual se entiende que debe ser castigado. Es más, el legislador español opta por incluir como hacking también las conductas de mantenimiento no autorizado en un sistema informático ajeno, a pesar de que gramaticalmente no se podrían entender propiamente como supuestos de acceso ilícito.

Optar por una regulación unitaria de los delitos informáticos es un acierto. Si se optara por un modelo similar, tipificando estas conductas en una norma, título o capítulo autónomo, delimitando claramente su bien jurídico protegido, estableciendo definiciones sobre los conceptos básicos y regulando a continuación el tipo básico y sus modalidades, sin duda ayudaría al intérprete en un campo tan complejo y en continuo cambio como el que se expone en este TFM, y podría evitar la mezcla de artículos y referencias que actualmente se encuentra en el Código Penal español sobre esta materia.

Con la reforma de 2015 se ha desaprovechado la oportunidad de separar claramente los delitos contra la intimidad y el hacking, incluso para establecer una regulación unitaria de los delitos informáticos, en la medida en que se ha elegido por dejar el contenido del anterior artículo 197.3 en el siguiente artículo, el 197 bis 1, dentro del mismo Capítulo. Sin embargo, esa nueva regulación debería ser un primer paso para una futura agrupación de estos delitos en un apartado propio del Código Penal, de tal forma que se consiga un tratamiento sistemático del precepto acorde con el bien jurídico protegido, facilitando su interpretación como ya ocurre en otros países.

Según se ha expuesto, el artículo 197 bis 1 presenta dificultades interpretativas por su ubicación sistemática. Por la descripción típica pudiera parecer que se trata de proteger la seguridad de los sistemas, como presupuesto para que la informática pueda desempeñar su función social, siendo necesaria su tutela y adelantando así la barrera de protección de otros bienes jurídicos.

Se ha de entender que la protección de los sistemas de información, comprendiendo la confidencialidad, integridad y disponibilidad, sin exigir su efectivo menoscabo, determina que es un delito de peligro concreto para la seguridad del sistema informático afectado.

En el nuevo artículo 197 bis 1 el acceso no autorizado a todo o parte de un sistema de información y la vulneración de las medidas de seguridad propuestas para que esto no suceda son los elementos que definen las conductas de hacking.

La colaboración público-privada es reconocida por todo el sector como el único camino de afrontar esta situación. La gestión de los riesgos, las amenazas, la prevención de estos elementos y el desarrollo de la capacidad de reacción ante una temprana alerta frente a incidentes se demuestra como estratégica en el mantenimiento de la integridad tanto de individuos como de empresas y estados. Nadie está excluido

del riesgo, por este motivo la necesidad de concienciación de estos riesgos es de cumplimiento obligado.

El estado actual de conciencia nacional de ciberseguridad es, al menos, sumamente mejorable. Esto no es de extrañar dado que el grado de compromiso de la sociedad española con la seguridad y defensa está muy lejos de ser el ideal y la ciberseguridad es un concepto que ha empezado a llegar al público no especializado hace relativamente poco tiempo.

Los procesos de convergencia de la ciberseguridad, ciberterrorismo, ciberespionaje y ciberactivismo hacen imprescindible el desarrollo en nuestro país tanto de capacitación personal como de afianzamiento empresarial de las compañías que realizan servicios en la prevención de todo este tipo de situaciones, tal y como están desarrollando los países de nuestro entorno. Entre las funciones que desarrollan, se encuentran la de proporcionar información de los riesgos y las amenazas del entorno global actual, ayudando así al responsable de la toma de decisiones a alertar sobre las tendencias y la información susceptibles de afectar a su organización.

Para alcanzar una reducción drástica del cibercrimen, la UE aboga por endurecer la legislación, desarrollando leyes específicas para «tipos de cibercrimen», junto con la creación de alianzas para su persecución. Por las características de los cibercrímenes, se requiere disponer de conocimientos especializados y medios tecnológicos para su investigación. Desde la UE se percibe un desequilibrio de capacidades entre los países miembros.

La formación, inicial y continua, desempeña por tanto un papel clave en la política pública de ciberinteligencia. Para que la iniciativa de ciberseguridad obtenga como consecuencia la toma de medidas apropiadas, se demanda formar a especialistas capaces de dirigir políticas de ciberinteligencia en las compañías y de elaborar las herramientas correspondientes.

Vivimos en un mundo complejo y contradictorio que está evolucionando cada vez más rápidamente, en el que el volumen y la multiplicidad de la información convierten a cada individuo, a cada empresa y a cada Estado en agente y árbitro de un juego que a menudo le supera. Sabemos más y más rápido y sobre más cosas, siendo conscientes, al mismo tiempo, de que la vulnerabilidad está en relación directa con el volumen del flujo de información recabado y de que la realidad virtual a veces gana por la mano a la verdadera.

Las conclusiones de este TFM van en línea con los tiempos actuales. Es necesario un planteamiento de concienciación en materias de ciberseguridad para la sociedad civil y para la Administración sobre de los riesgos que les amenazan. La colaboración de las diferentes Administraciones Públicas y de la sociedad civil es necesaria y fundamental para la formación de una conciencia nacional de ciberseguridad.

En estos momentos, los ciudadanos y muchas empresas poseen intereses que defender frente al cibercrimen, sobre todo fraudes, estafas, robo de información, acoso, incluida información comprometedora, y otras amenazas del estilo, pero se encuentra muy poco interés en la defensa colectiva de los intereses comunes. Además, como se ha manifestado con anterioridad, hay poca conciencia de las amenazas que rodean como colectividad en el ciberespacio y menos aún de que los usuarios pueden ser usados por esas amenazas para encubrirse.

Con el fin de desarrollar una conciencia de ciberseguridad, es necesario conocer las amenazas y los riesgos y asumirlos, en el sentido de aceptarlos y enfrentarlos, no en el sentido de conformidad y pasividad ante los mismos. Comunicar las incidencias, formar en materias de seguridad cibernética y la necesaria adaptabilidad de usuarios, instituciones y empresas a las circunstancias cambiantes del ciberespacio.

Los centros docentes juegan un papel sumamente importante en la creación de conciencia de ciberseguridad, que será nacional cuando alcance a la mayor parte de la población. Para conseguir la participación de los docentes, es necesario primero concienciarlos y formarlos en ciberseguridad, aunque los resultados de la actividad de las instituciones de enseñanza han de verse a medio y largo plazo. La conciencia de ciberseguridad puede plasmarse en buenas prácticas informáticas o en algo más amplio que podría llamarse ciberurbanidad o cibereducación y que sería una extensión de las normas y usos de la buena educación al ciberespacio.

Si se buscan resultados a corto plazo, es primordial que las instituciones y los medios de comunicación se involucren. Para ello es necesario que los dirigentes de esas instituciones se conciencien de la necesidad de la ciberseguridad. En cuanto a los medios de comunicación, los dirigentes tienen un doble papel aquí, concienciarse y concienciar al personal que trabaja en sus medios.

Los mensajes de concienciación de seguridad necesitan ser adaptados al público objetivo. Para asegurar que los mensajes son relevantes, que se han recibido y entendido, se debe tener en cuenta las particularidades de cada organización y su entorno de trabajo.

Una vez que esta labor de concienciación se lleve a cabo, tanto ciudadanos comunes como organizaciones serán capaces de detectar a su nivel las amenazas y evadirlas o contrarrestarlas.

13.GLOSARIO.

Amenaza: Dicho o hecho con que se amenaza.

Bien jurídico protegido: En derecho penal, bien tutelado por el Estado con ocasión de la tipificación de una determinada conducta como delito o falta.

Ciberdelito: aquella acción antijurídica que tiene como objetivo destruir y dañar activos, sistemas de información u otros sistemas de computadoras, utilizando medios electrónicos y/o redes de Internet en la cual se determina que el acusado es culpable.

Ciberespacio: Espacio virtual creado con medios cibernéticos.

Concienciación: Acción y efecto de concienciar o concienciarse.

Hacker: Persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos.

Hacking: búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo.

Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Legislación: Conjunto de leyes por las cuales se regula un Estado o una actividad determinada.

Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas

14.BIBLIOGRAFIA.

ANARTE BORRALO, E., MORENO MORENO, F. y GARCÍA RÚIZ, C. (Coordinadores), Nuevos conflictos sociales. El papel de la privacidad, ed. Iustel, Madrid, 2015.

ANARTE BORRALLO, E y DOVAL PAÍS, A., "Efectos de la reforma de 2015 en los delitos contra la intimidad", en Diario La Ley, nº 8744, 19 de abril de 2016.

Bermúdez González, J.A., Descubrimiento de secretos e intrusiones informáticas. Centro de Estudios Jurídicos, Madrid 2016.

Ciberseguridad y el nuevo Código Penal. Madrid. Ateinco. [Consulta 8 de abril de 2019].<https://www.ateinco.com/ciberseguridad-y-el-nuevo-codigo-penal/>

Colás Turégano, A. El delito de intrusismo informático tras la reforma del CP español de 2015. Revista Boliviana de Derecho Nº 21, Enero 2016, pp. 210-229.

DE LA MATA BARRANCO, N. J., Derecho penal europeo y legislación española: las reformas del Código penal. Ed. Tirant lo Blanch, Valencia, 2015.

Delitos contra la intimidad. Madrid. Tu Abogado Defensor. [Consulta 10 de abril de 2019].< https://www.tuabogadodefensor.com/delitos-contra-la-intimidad/>

DELITOS INFORMÁTICOS - Ataques que se producen contra el derecho a la intimidad. Sevilla. [Consulta 10 de abril de 2019].<http://www.portaley.com/delitos-informaticos/codigo-penal-197-201.shtml>

Derecho Penal y Criminología. Madrid. UNED. [Consulta 5 de abril de 2019].<http://espacio.uned.es/fez/eserv/bibliuned:revistaDerechoPenalyCriminologia-2015-13-7010/pag_51.pdf>

Descubrimiento y revelación de secretos. Barcelona. Wolter Kluwer. [Consulta 01 de abril
2019].<http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUMjE0MztbLUouLM_DxbIwMDCwNzAwuQQGZapUtckhIQaptWmJOcSoA8d8oDjUAAAA=WKE>

El delito de intrusismo informático tras la reforma del CP español de 2015. Bolivia. Iuris Tantum Revista Boliviana de Derecho. [Consulta: consulta 1 de abril de 2019] <http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572016000100010>

GONZÁLEZ CUSSAC, J.L, CUERDA ARNAU, M.L., FERNÁNDEZ HERNÁNDEZ, A. Y OTROS. Nuevas amenazas a la Seguridad Nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación. Tirant lo Blanch, Valencia 2013.

GONZÁLEZ CUSSAC, J. L., "Estrategias legales frente a las ciberamenazas", en Cuadernos de estrategia (Ministerio de Defensa), ed. Ministerio de Defensa: Instituto Español de Estudios Estratégicos, nº 149, Madrid, 2011.

GONZÁLEZ RUS, J. J., "La criminalidad organizada en el Código Penal Español. Propuestas de reforma", en Anales de derecho, nº 30, ed. Universidad de Murcia, Murcia, 2012, disponible en http://revistas.um.es/analesderecho/article/view/161841/142081, consultado el 9 de abril de 2017.

Los nuevos “delitos informáticos” tras la reforma del código penal. Murcia. [Consulta 9 de abril de 2019]. <http://www.legaltoday.com/practica-juridica/penal/penal/los-nuevos-delitosinformaticos-tras-la-reforma-del-codigo-penal>

MORILLAS CUEVA, L. (director) y otros, Estudios sobre el Código Penal reformado (Leyes Orgánicas 1/2015 y 2/2015). Dykinson, Madrid 2015.

MIRÓ LLINARES, F., El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio, ed. Marcial Pons, primera edición, Madrid, 2012.

RUEDA MARTÍN, M. Á., “Los ataques contra los sistemas informáticos: conductas de hacking. Cuestiones político-criminales”, en ARMAZA ARMAZA, Emilio José (Coord.), y VVAA, La Adaptación del Derecho Penal al Desarrollo Social y Tecnológico, ed. Comares, Granada, 2010.

Siete delitos contra la privacidad e intimidad (I). Sevilla. Garberi Penal. [Consulta: 29 de marzo de 2019] <http://www.garberipenal.com/siete-delitos-contra-la-privacidad-e-intimidad/ >